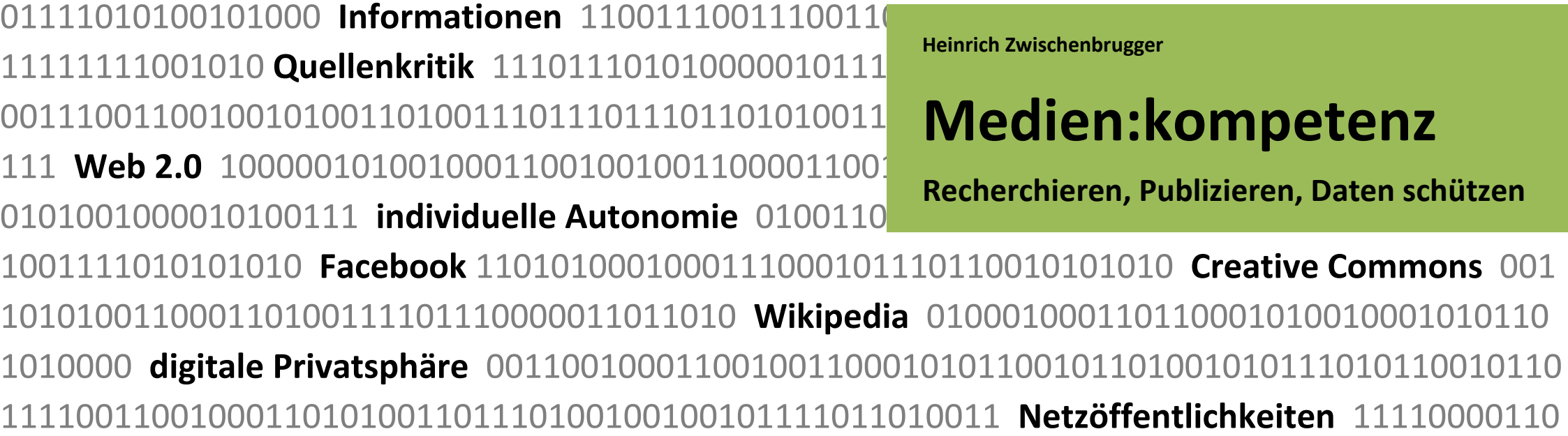


Heinrich Zwischenbrugger

Medien:kompetenz

Recherchieren, Publizieren, Daten schützen

Heinrich Zwischenbrugger
St.-Pankratius-Gasse 9/a
I-39020 Glurns
E-Mail: zwi@posteo.net

OpenPGP Public-Key
Key Fingerprint: B388 E936 FF7A C277 41D0 C912 FE30 BFEC 3AD3 8A06
Ablauf-Datum: 08.05.2024

Kritik und Anregungen sind jederzeit willkommen.

Die Publikation steht unter der Creative Commons-Lizenz 3.0 Italien: https://creativecommons.org/licenses/by-nc-nd/3.0/it/. Das Werk darf in der vorliegenden Form bei Namensnennung des Autors zu nicht kommerziellen Zwecken genutzt und es darf nicht bearbeitet oder in anderer Weise verändert werden.

Der Autor ist Lehrer für Recht und Ökonomie an der Fachoberschule für Wirtschaft (FOWI)-Mals/Italien.

Die Fotos stammen vom Autor selbst.

Inhalt

Einführung 5

1 Richtig recherchieren 7

1.1 Informationen suchen 8
1.1.1 Informationsbedarf feststellen 8
1.1.2 Recherche in Bibliothekskatalogen 10
1.1.3 Suche nach E-Books 12
1.1.3.1 E-Book-Angebote 12
1.1.3.2 Kopierschutztechniken 13
1.1.3.3 E-Book-Formate 15
1.1.4 Suche im Internet 16
1.1.4.1 Suchmaschinen 16
1.1.4.2 Techniken der Suchabfragen 20
1.1.4.3 Spezielle Suchdienste und Spezialsuchmaschinen 25
1.1.5 Lokale Websuche 25
1.1.6 Suche in Wikipedia 26
1.1.6.1 Die Funktionsweise von Wikipedia 26
1.1.6.2 Wikipedia richtig nutzen 28
1.1.7 Recherche 2.0 31
1.1.8 Sicher recherchieren 32
1.2 Informationen beurteilen 34
1.2.1 Recherche, Vertrauen und Skepsis 34
1.2.2 Bewertungskriterien 36
1.3 Informationen festhalten 39
1.4 Auf dem Laufenden bleiben 42
1.5 Arbeitsaufträge 45

2 Digitales Publizieren und Recht 53

2.1 Das Urheberrecht 54
2.1.1 Schutz des Urhebers 54
2.1.1.1 Wer ist Urheber? 54
2.1.1.2 Welche Rechte hat der Urheber? 55
2.1.1.3 Was ist das Hausrecht? 56

2.1.2 Schutz des Nutzers 57
2.1.2.1 Interessen im Urheberrecht 57
2.1.2.2 Privatkopie 57
2.1.2.3 Zitate und Links 59
2.1.2.4 Schulgebrauch 62
2.1.2.5 Öffentliches Informationsinteresse 62
2.1.3 Creative Commons – Lizenz fürs Internet 63
2.1.4 Rechtsrahmen der Medienwerkstatt 67
2.1.4.1 Texte 68
2.1.4.2 Fotos 70
2.1.4.3 Videos 76
2.1.4.4 Audios 76
2.1.4.5 Online-Schülerzeitung 79
2.2 Der Datenschutz 82
2.2.1 Schutz durch Recht 83
2.2.2 Schutz durch Technik 86
2.2.2.1 Metadaten in Word-Dateien 86
2.2.2.2 Metadaten in PDF-Dateien 89
2.2.2.3 Metadaten in Audio-Dateien 90
2.2.2.4 Metadaten in Foto-Dateien 90
2.3 Eigene oder fremde Webseite? 93
2.3.1 Eigene Webseite 93
2.3.2 Fremde Webseite 93
2.4 Arbeitsaufträge 95

3 Facebook klug nutzen 101

3.1 Was ist Facebook? 101
3.2 Facebook-Konto anlegen 103
3.3 Facebook-Funktionen 105
3.4 Wie schützt du deine Privatsphäre? 107
3.4.1 Das Profil – Das virtuelle „Ich“ 107
3.4.2 Privatsphäre-Einstellungen anpassen 108
3.5 Rechtliches für Inhalte in Facebook 114
3.5.1 Urheber- und Persönlichkeitsrecht 114
3.5.2 Impressumspflicht 116
3.6 Umgang mit Cybermobbing 116
3.6.1 Was ist Cybermobbing? 116
3.6.2 Schutz vor Cybermobbing 118

3.7 Problemfälle und Alternativen 120
3.8 Arbeitsaufträge 126

4 Smartphone sicher nutzen 131

4.1 Abschluss eines Handyvertrages 132
4.2 Grundrecht auf vertrauliche Telekommunikation 133
4.2.1 Überwachung durch Polizei 133
4.2.1.1 Wann darf überwacht werden? 133
4.2.1.2 Wie läuft die Überwachung ab? 134
4.2.2 Überwachung durch NSA & Co. 137
4.2.2.1 Was erlaubt das Völkerrecht? 138
4.2.2.2 Schutzinstrumente vor Cyberspionage 139
4.2.3 Sicherheit vs. Privatsphäre 141
4.3 Die Smartphone-Sicherheitseinstellungen 142
4.4 Vorsicht bei Apps 145
4.4.1 Apps als Datensammler 145
4.4.2 Schutz vor Schnüffel-Apps 145
4.5 Schutz vor Viren & Co 147
4.6 Schutz der Privacy 149
4.6.1 Betriebssystem und lokale Daten verschlüsseln 150
4.6.1.1 Android verschlüsseln 150
4.6.1.2 Lokale Daten verschlüsseln 151
4.6.2 Datenverkehr verschlüsseln 153
4.6.2.1 Chat verschlüsseln 153
4.6.2.2 Cloud verschlüsseln 154
4.6.2.3 Telefonat verschlüsseln 159
4.6.2.4 E-Mails verschlüsseln 159
4.6.3 Passwortmanager 163
4.6.4 Daten sicher löschen 166
4.7 Schutz der Verfügbarkeit 168
4.8 Schutz der Anonymität 169
4.9 Handy-Tipps, Plattformen, Apps 172
4.10 Arbeitsaufträge 179

5 Von der Medienkompetenz zum Mediendiskurs 185

5.1 Digitalisierung des Alltags 185
5.2 Netz-Ökonomie 187
5.3 NSA & Co. im Netz 189
5.4 Web 2.0-Diskurs 192

Glossar/Abkürzungen 194

Literatur 209

Einführung

Das Leben in der Gesellschaft ist heute durchdrungen von Medien- und Kommunikationstechnik. Um Konsument und Produzent in der Informationsgesellschaft zu sein, ist Medienkompetenz unabdingbar. Medienkompetenz heißt aber mehr als Bedienkompetenz. Das Spektrum der Medienkompetenz reicht von der Basiskompetenz, etwa mithilfe eines Office-Programmes einen Geschäftsbrief zu schreiben, bis zur Fähigkeit, im Internet nach verlässlichen Informationen zu recherchieren, eigene Blogs, Texte, Fotos oder Videoclips zu publizieren. Medienkompetenz ist eine wichtige Voraussetzung dafür, im Umfeld einer digitalisierten Wissensgesellschaft ein selbstbestimmtes Leben führen zu können. Selbstbestimmt sein heißt, fähig zu sein, den eigenen Willen handlungswirksam zu realisieren, also zu wissen, wie’s geht. Zur Medienkompetenz gehört auch Urteilskraft, also die Fähigkeit, eigene Entscheidungen informiert, überlegt zu treffen und die Folgen der eigenen Handlungen einschätzen zu können.

Medienkompetenz ist keine Komplizin der „schönen neuen Medienwelt“, sondern fördert den kritischen, autonomen Umgang mit den neuen Medien. Der autonome Nutzer weiß nicht nur, wie man im Internet Informationen erschließen oder selbst bereitstellen kann, sondern fragt auch nach den Auswirkungen der neuen Medien auf Freiheit, Sicherheit und Demokratie. So kann sich etwa die Frage stellen, inwiefern das Urheberrecht die Interessen der Kreativen, der Vermarkter oder der Nutzer schützt. Ökonomische Gesichtspunkte spielen ebenso eine Rolle. Wie funktioniert der Medienmarkt? Gibt es auf dem Medienmarkt einen wirksamen Wettbewerb oder beherrschen Oligopole den Markt? Was sind die wirtschaftlichen Hintergründe der Gratisangebote im Netz? Die hier verstandene Medienkompetenz pendelt zwischen den Polen Aufklärung, Web 2.0-Kompetenz und informierter und offener Diskussion. Leitidee ist die „digitale Selbstständigkeit“. Damit ist der selbstbestimmte Nutzer gemeint, der die neue Medienwelt versteht, zielgerichtet nutzt und Alternativen kennt, wie er in der digitalen Welt seine Pläne realisieren könnte. Medienkompetenz bietet für alle die Chance, an der Wissensgesellschaft zu partizipieren.

Die vorliegende Arbeit ist eine praxisorientierte Einführung in die Medienkompetenz. Die Arbeit befasst sich mit den Themen Recherchieren und Publizieren im Internet, mit der sozialen Plattform Facebook sowie mit Sicherheitsfragen rund um das Smartphone. Jedem Kapitel sind Leitfragen vorangestellt, die dich mit den grundlegenden Fragestellungen des Sachgebietes vertraut machen sollen. Im laufenden Text findest du Tipps, die du als Faustregeln für die tägliche Mediennutzung verwenden kannst. Abbildungen sollen den Text auflockern, dir aber auch helfen, auf „einen Blick“ einen Zusammenhang zu erkennen oder eine Abfolge in einer Schritt-für-Schritt-Anleitung zu illustrieren. Die Arbeitsaufgaben am Ende der einzelnen Kapitel

dienen der Überprüfung und Vertiefung des erarbeiteten Sachgebiets und sind als Anregung zu verstehen, die Medienkompetenz um weitere Handlungsfelder zu ergänzen, zu vertiefen und zu reflektieren.

In dieser Arbeit wurde meist die männliche Form gewählt, wenn es um Nutzerinnen oder Nutzer ging. Natürlich sind stets weibliche und männliche Personen gleichermaßen gemeint. Ohne Fachbegriffe kommt keine Medienkompetenz aus. Im Glossar wird knapp erklärt, was die gängigen Fachbegriffe bedeuten. Die Einführung hat eine Schlagseite: Die Anwendungen beziehen sich nur auf das Windows 7- und Android-Betriebssystem 4.4.2.

Glurns, August 2015

1 Richtig recherchieren

Leitfragen

- Wie findet man die relevanten Suchbegriffe für die Recherche?
- Warum soll man für die Suche immer mehrere Suchwerkzeuge benutzen?
- Welche Werkzeuge der Suchabfragen gibt es?
- Welche Kriterien gibt es für die Bewertung der Suchergebnisse?
- Wie kannst du die Qualität der Informationen bei Wikipedia überprüfen?
- Mit welchen Hilfsmitteln kannst du die Suchergebnisse festhalten?
- Wie kannst du zu deinem Recherchethema auf dem Laufenden bleiben?

Sorgfältige Recherche zählt zu den Schlüsselkompetenzen in der Informationsgesellschaft und sollte deshalb zu den Kernkompetenzen der schulischen Bildung gehören. Was heißt aber Recherchieren? Unter Recherchieren versteht man nicht nur die Kompetenz die benötigten Informationen[1] zu finden, sondern auch diese zu überprüfen, kritisch zu bewerten, festzuhalten sowie zu einem bestimmten Sachgebiet auf dem Laufenden zu bleiben. Ist der Schüler in der Lage, autonom zu recherchieren, wird er die Qualität der Informationen hinterfragen und nicht blind einer Twitter-Meldung vertrauen oder ungeprüft eine neue App auf seinem Handy installieren. Das Web ermöglicht zudem, dass Nutzer sich auch untereinander verbinden können, wenn sie ähnliche Fragen haben.

Die sorgfältige Recherche bildet auch die Grundlage für das Grundrecht auf Meinungs- und Pressefreiheit (Art. 21 Verf., Art. 10 EMRK). Denn die kritische Öffentlichkeit nimmt nur solche Stellungnahmen ernst, die sich auf handfeste Informationen stützen können. Belegbare Informationen eines Journalisten oder eines Bloggers bewegen mitunter mehr als weltfremde politische Visionen. Der vernünftige öffentliche Austausch von Informationen und Argumenten setzt voraus, dass auch Bürger kompetent recherchieren können.

1 Was genau der Begriff Information bedeutet, ist umstritten. In jedem Fall gibt die Information eine Antwort auf Fragen wer? was? wo? wann? wie? warum? mit wessen Hilfe? Informationen liegen in einer übertragbaren Form vor, sie können eine verbale, schriftliche, bildhafte oder digitale Form aufweisen; vgl. „Information“. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 7. Juni 2015, 03:00 UTC. URL: http://de.wikipedia.org/w/index.php?title=Information&oldid=142860395 (Abgerufen: 11. Juni 2015, 16:48 UTC); http://www.minet.uni-jena.de/dbis/veranstaltungen/2004/wedekind/wedekind-festvortrag.pdf

Recherchekompetenz ist eine neue Kulturtechnik, die im Beruf und Alltag weiterhilft. Nur wer informiert ist, kann in allen problematischen Situationen eine begründete, bewusste Entscheidung treffen und hat die Chance, die gesetzten Ziele zu erreichen und somit die eigenen Lebensumstände selbst zu bestimmen. Das Internet ermöglicht uns, das „Wissen der Welt“ lesend, hörend und sehend per Mausklick oder Fingertipp zu erschließen. Beim Suchen, Bewerten oder Sichern von Informationen kannst du Techniken und digitale Assistenten einsetzen, die wir in diesem Kapitel vorstellen wollen.

1.1 Informationen suchen

1.1.1 Informationsbedarf feststellen

Am Anfang einer jeden Recherche steht die Erkenntnis, dass man etwas nicht weiß und etwas wissen will. Ist der konkrete Informationsbedarf aber so ohne Weiteres einfach zu erkennen? Das hängt von der Fragestellung ab. Willst du lediglich nach der nächsten Zugverbindung suchen oder den Straßenpreis eines bestimmten Smartphones wissen, ist klar, was du suchst. Sollen Schüler hingegen in einem Workshop interessierten Eltern zeigen, wie man PCs und Smartphones sichert, dann kann der spontane Informationsbedarf zu schnell als gedeckt angesehen werden.

Zunächst müssen die Erwartungen geklärt werden, die mit der Recherche verknüpft sind. Wie umfassend muss das Thema ausgearbeitet werden? Bis wann muss die Arbeit abgeliefert werden? Was sind die Bewertungskriterien? Welche Erwartungen hat Lehrer? Welche Wissenschaftler? Oder welche sind in Gesetzen festgehalten? Eine IT-Firma, die beispielsweise Smartphones per Iris-Scan kombiniert mit Aderscan entsperren will, wird in jedem Fall eine umfassende und sorgfältige Patentrecherche vornehmen, will sie nicht eine kostspielige Patentklage der Mitbewerber riskieren und so an der Einführung der technischen Innovation gehindert werden und vielleicht

Art. 10 EMRK

„(1) Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben.“

„Ich weiß, dass ich nichts weiß.“

Sokrates, griechischer Philosoph

Recherche-Thema: Smartphone sichern

- Wie kann man das Smartphone vor unberechtigten Zugriffen schützen?
- Welche Virenprogramme schützen das Smartphone effektiv vor Schadcode?
- Wie erstellen Nutzer sichere Passwörter mithilfe eines Passwortgenerators?
- Welche Apps gibt es zur verschlüsselten Kommunikation (telefonieren, chatten, sms, mailen)?
- Wie finden Nutzer heraus, auf welche Smartphone-Daten Apps zugreifen?
- Wo hinterlassen User beim Surfen und Kommunizieren im Netz Daten?
- Wie können Nutzer ihre IP-Adresse beim Surfen verschleiern?
- Mit welchen Tools kann man anonym surfen?
- Wie können Anwender ihre Daten und Apps wirksam schützen?

auch am Rande der Zahlungsunfähigkeit stehen.

Im nächsten Schritt muss die Recherche sinnvoll eingegrenzt werden. Erst wenn der Schwerpunkt der Recherche geklärt ist, können zielführende Fragestellungen formuliert werden. Ohne klare Abgrenzung des Themas, kann man später nicht entscheiden, ob eine Information oder ein Dokument noch relevant ist oder unbesehen übergangen werden kann. Um abzuklären, was zu einem Thema gehört und was nicht, ist ein Blick in Wikipedia meistens nützlich. Wikipedia-Artikel eignen sich für die schnelle Recherche über ein Thema. Auf der Wikipedia-Hauptseite findest du den Link *Themenportale.* Steuerst du die Themenportale an, so erscheint eine Übersicht zu verschiedenen Themenbereichen. Innerhalb eines Themenbereichs sind die wichtigsten Artikel zum Themengebiet aufgelistet. Die Portale sind eine gute Anlaufstelle, wenn man größere Zusammenhänge überblicken möchte. Einen schnellen Überblick über ein neues Themengebiet verschaffst du dir auch mit der Suchhilfe Wikimindmap.[2] Willst du dich beispielsweise über das Themengebiet Datenschutz informieren, rufst du die Suchhilfe auf und wählst unter *Select a Wiki* die deutsche Wikipedia aus (de.wikipedia.org) und gibst hinter *Enter your Topic* den Begriff *Datenschutz* ein. Wikimindmap durchsucht die ausgewählte Wikipedia und zeigt das Ergebnis als Mindmap an. Klickst du auf das Pluszeichen am Ende eines Astes, öffnet sich ein weiterer Ast. Mit einem Klick auf die grünen Pfeile wird eine neue Mindmap generiert mit dem jeweiligen angeklickten Stichwort im Mittelpunkt. Für vertiefende Informationen reicht Wikipedia nicht aus. Studenten etwa, die zum Abschluss ihres Studiums eine Magisterarbeit schreiben, wählen als Einstieg in ein Thema allgemeine Nachschlagewerke wie Handbücher, Enzyklopädien oder Lehrbücher.

Wie gehst du am besten vor, um dich über das Themengebiet „IT-Grundschutz von PCs und Smartphones“ zu informieren? Plattformen für IT-Sicherheit sind hilfreiche Anlaufstellen, um einen Überblick über das Themengebiet zu gewinnen. Erstelle eine Mindmap[3], denn mit ihrer Hilfe kannst du die Gedanken zum Thema ordnen und herausfinden, welche Informationen du für den Workshop noch benötigst. Eine Mindmap kann sichtbar machen, dass noch Informationsbedarf zu den Punkten „sichere Passwörter und kostenlose Passwortmanager für Windows-PCs und Android-Smartphones“ besteht. Ist geklärt, in welche Richtung die Recherche gehen soll, dann mache dir Gedanken über die Struktur deines Themas. Steht die Struktur, kann sie mit Informationen gefüllt werden.

Hast du festgelegt, nach was du suchst, musst du nun überlegen, wo die gesuchte Information veröffentlicht sein könnte. Nach Informationen suchen kannst du in lokalen Bibliotheken, in Bibliothekskatalogen oder im Internet.

2 http://www.wikimindmap.org/
3 Mit dem kostenlosen Open-Source-Tool FreeMind kannst du Mindmaps erstellen, die mit Texten und Bildern versehen werden können: http://freemind.sourceforge.net/wiki/index.php/Main_Page

1.1.2 Recherche in Bibliothekskatalogen

Verfügst du bereits über eine Literaturliste zum Thema Passwortmanager, musst du nur noch über den lokalen, regionalen, überregionalen Bibliothekskatalog oder über Metakataloge nach der benötigten Literatur suchen. Über eine gezielte Recherche in Bibliothekskatalogen kannst du ermitteln, ob sich der gesuchte Titel im Bestand einer bestimmten Bibliothek befindet.

Fehlen Literaturtipps von der Lehrkraft oder reichen sie für die Ausarbeitung des Themas nicht aus, dann musst du dir die passenden Suchbegriffe zusammenstellen. Erstelle dazu kurze, aussagekräftige Sätze oder Fragen und filtere daraus die Begriffe heraus, die das Sachgebiet charakterisieren. Ergänze in einem nächsten Schritt diese Begriffe mit Ober- und Unterbegriffen, mit sinnverwandten Wörtern und mit unterschiedlichen Schreibweisen. Auf diese Weise erhältst du eine Schlagwortliste für deine Suche in Bibliothekskatalogen.

Tipp

Auch bei Suchanfragen in Bibliothekskatalogen gilt der Grundsatz „Weniger ist mehr!“ beachten. Gib bei bekannten Titeln nur den Nachnamen des Autors und ein sinntragendes Wort aus dem Titel ein, z. B. die Suchwörter *Friedrich* und *Vernunft* für den Buchtitel: Jörg Friedrich: *Kritik der vernetzten Vernunft. Philosophie für Netzbewohner*, Hannover 2012. Zu viele Wörter begrenzen die Suche und führen vielfach zu schlechten Suchergebnissen.

Bezeichnung der Bibliothek	Webadresse
(biSon) Bibliotheken Südtirols Online (Verbundkatalog der öffentlichen Bibliotheken in Südtirol)	http://bib2.provinz.bz.it/bisonii/app/pages/webopac/index.aspx
(biS) Sistema Biblioteche (Verbundkatalog der italienischen Bibliotheken Südtirols)	http://www.provinz.bz.it/cultura/bis.htm
Landesbibliothek Dr. Friedrich Tessmann	http://www.tessmann.it
BIBLIO 24 Südtirols Online Bibliotheken	http://www.biblio24.it
MetaOPAC	http://pro.unibz.it/opacuni/
OPAC SBN Catalogo del Servizio Bibliotecario Nazionale	http://www.sbn.it/opacsbn/opac/iccu/free.jsp
KVW Karlsruher Virtueller Katalog	http://kvk.uni-karlsruhe.de
Europeana – Europas digitale Bibliothek	http://www.europeana.eu/
WorldCat - weltweiter Verbundkatalog von über 10.000 Bibliotheken	http://www.worldcat.org

Tab. 01: Lokale und überregionale Bibliothekskataloge

Bibliothekskataloge bieten in der Regel für Recherchen sowohl eine einfache als auch eine erweiterte Suche an. Wenn du beispielsweise die Startseite der Tessmann-Bibliothek[4] aufrufst, erscheint die Suchmaske für die Einfache Suche. Bei der einfachen Suche werden die wichtigsten Suchfelder durchsucht: Autor, Titel und Schlagworte. Klickst du auf die Schaltfläche *Erweiterte Suche*, öffnet sich eine Suchmaske mit mehreren Suchfeldern: *Titel, Autor, Erscheinungsjahr, Schlagwort, Notation, Körperschaft*. Du kannst nun deine Recherche nach formalen Merkmalen, wie Autor, Titel usw. oder nach einem bestimmten Thema durchführen. Weißt du, welches Buch oder welchen Artikel du benötigst, gibst du in die entsprechenden Felder Titel und Autor ein und prüfst, ob der gesuchte Titel im Bibliotheksbestand geführt wird und ob er zurzeit ausleihbar ist.

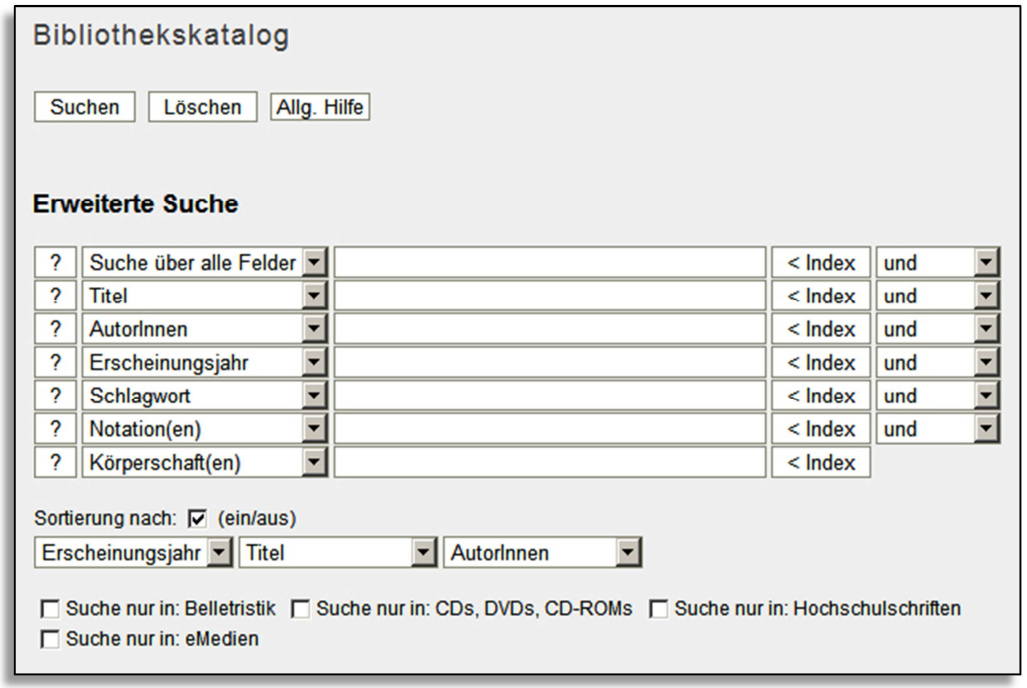


Abb. 01: Erweiterte Suche im Tessmann-Bibliothekskatalog

Musst du erst herausfinden, welche Literatur in der Tessmann-Bibliothek zu einem Thema vorhanden ist, ist die Schlagwortsuche die bessere Option. Bei der Schlagwortsuche handelt es sich nämlich um eine thematische Suche. Die Suche wird auf Begriffe begrenzt, die zur inhaltlichen Beschreibung der Publikation passen. Hast du Zweifel, welche Schlagwörter in der Datenbank der Bibliothek tatsächlich verwendet werden, dann gibst du zumindest die ersten 3 Buchstaben des Suchbegriffs in das Suchfeld ein und klickst auf *Index*. Über den *Index* kannst du erfahren, ob es im Umfeld des gewählten Schlagwortes weitere relevante Schlagwörter gibt. Die gelisteten Schlagwörter sind mit den einzelnen Publikationen verknüpft. Mit einem Klick auf ein Schlagwort werden die mit dem Schlagwort verbundenen Publikationen in einer Kurztitelliste angezeigt. Mit einem weiteren Klick auf den einzelnen Titel erscheint der komplette Eintrag der Publikation, also Autor, Titel, Erscheinungsjahr, ISBN, Schlagwort, Signatur und Exemplar.

Suchanfragen führen nicht immer zum gewünschten Erfolg. Der Grund dafür kann in einer falschen Suchanfrage liegen oder darin, dass weder regionale noch große Bibliotheken alle Publikationen zu bestimmten The-

4 http://www.tessmann.it

men verfügbar haben können. Weiterhelfen kann in einem solchen Fall eine Recherche bei einem Buchshop, Online-Antiquariat oder im Netz. Ein Teil der Publikationen ist weder von Bibliotheks- noch von Buchkatalogen der Online-Shops erfasst, sondern ist nur mehr im Netz als digitale Publikation abrufbar.

1.1.3 Suche nach E-Books

Ein stetig zunehmender Teil der Information erscheint nur mehr als E-Book. Vielfach werden parallel zum Buch aus Papier auch digitale Bücher publiziert. Aber nicht jedes E-Book beruht zwangsläufig auf einem gedruckten Buch. Die gesuchten Informationen könnten sich also auch nur in E-Books befinden. Werfen wir also einen Blick auf E-Books und ihre Besonderheiten.

1.1.3.1 E-Book-Angebote

E-Books werden über Verlage, spezialisierte E-Book-Portale oder direkt vom E-Book-Autor über das Internet angeboten. Die Angebote der Verlage und der E-Book-Portale sind in der Regel kostenpflichtig. Kostenlos sind gemeinfreie Bücher, deren Urheberrecht bereits abgelaufen ist, oder Bücher, die Autoren aus Gründen der Aufmerksamkeit gratis anbieten.

Checkliste E-Book-Portale

- Welches Portal hat das größte Sortiment an E-Books?
- In welchen Dateiformaten werden die E-Books angeboten?
- Mit welchem Kopierschutz sind E-Books versehen? Adobe-DRM oder Wasserzeichen-DRM?
- Welche Lesegeräte unterstützt das E-Book-Portal?
- Unterliegen die E-Books einer persönlichen oder einer CC-Lizenz?
- Welche Nutzerdaten werden an das E-Book-Portal gesendet: die Gerätekennung des E-Book-Readers, das Leseverhalten, die markierten Stellen, die hinterlegten Notizen?
- Was macht das E-Book-Portal mit den Nutzerdaten? Werden sie verkauft oder für Werbung verwendet?
- Wie lauten Anschrift, Rechtsform und Gerichtsstand des E-Book-Portals?

E-Books sind heute auch Bestandteil des digitalen Angebots vieler öffentlicher Bibliotheken. Die Ausleihe von E-Books ist nicht nur für Schüler und Studenten eine Alternative. Unter der Ausleihplattform Onleihe[5] findest du digitale Bibliotheken aus Deutschland, Österreich, Schweiz und Südtirol.[6] Du kannst auf den Online-Bibliotheken nicht nur nach E-Books, sondern auch nach weiteren digitalen Medien, wie E-Paper, E-Musik, E-Audio oder E-Videos suchen, diese ausleihen und herunterladen. Kosten für die Ausleihe fallen keine an. Die Leihfrist für E-Books ist zeitlich befristet – so wie bei Printausgaben.

5 http://www.onleihe.net/
6 BIBLIO 24 ist ein Verleihverbund Südtirols Online-Bibliotheken: http://www.biblio24.it. Anmelden kannst du dich nur als bereits registrierter Benutzer einer Bibliothek vor Ort.

E-Book-Portale	Webadresse	Besonderheiten
Amazon	http://www.amazon.com	Amazon ist ein kommerzieller Anbieter, hat aber auch kostenlose E-Books im Sortiment.
Bookboon	http://bookboon.com/de	Bookboon bietet kostenlose E-Books für Studium und Beruf an.
Google Books	http://books.google.de	Google Books bietet kostenlose E-Books an, die nur online gelesen werden können. Sie können nicht auf Lesegeräte heruntergeladen werden.
MobileRead Wiki	http://wiki.mobileread.com/wiki/Free_eBooks	MobileRead Wiki listet Bezugsquellen für kostenlose E-Books auf.
Project Gutenberg	http://www.gutenberg.org	Project Gutenberg bietet mehr als 46.000 kostenlose E-Books an. Die E-Books können online gelesen oder heruntergeladen werden.

Tab. 02: Suche nach kostenlosen E-Books

1.1.3.2 Kopierschutztechniken

Beim Kauf eines E-Books erwirbt der Käufer nur die persönliche Lizenz das E-Book zu nutzen – kein Eigentum am E-Book als Datei. Die Nutzer-Lizenz erlaubt nicht, das E-Book zu verkaufen, zu verschenken oder zu verleihen. Gefällt das E-Book nicht, kann es nicht umgetauscht werden, ist die Lese-Hardware ungeeignet, kann es nicht mehr zurückgegeben werden. Ein sog. Digital Rights Management (DRM) soll sicherstellen, dass die E-Book-Käufer das Buch nur persönlich nutzen. Den Käufern ist es gesetzlich verboten, den technischen Kopierschutz zu umgehen.[7]

„Harter“ Kopierschutz

Zum „harten“ Kopierschutz zählt das Adobe-DRM. Hier definiert die Technik die Rechte des Nutzers, etwa wie oft dieser das E-Book auf unterschiedlichen Lese-Geräten kopieren darf oder wann die Ausleihzeit für das E-Book endet. In der Regel wird als harter Kopierschutz das Adobe-DRM verwendet.[8] Wie musst du vorgehen, um E-Books auf dem PC, Smartphone oder E-Book-Reader lesen zu können?

7 Vgl. Artt. 71-sexies, 102-quater, 171-ter L 633/1941
8 Apple und Amazon bieten E-Books über eine eigene harte DRM-Technik an. E-Books von Amazon können nur mit dem Kindle oder mit der Kindle-Software angezeigt werden.

Zunächst musst du eine Adobe-ID anlegen. Die Adobe-ID ist dein digitaler Identitätsausweis. Rufe dazu die Adobe-Webseite[9] auf und klicke auf den Link „Sie sind noch nicht Mitglied? Adobe-ID erstellen“. Fülle das Eingabeformular aus und folge den Anweisungen auf der Webseite. Die bei Adobe angegebene E-Mail-Adresse bildet deine persönliche Adobe-ID. In einem zweiten Schritt musst du eine Lese-Software installieren, um E-Books lesen zu können. Wähle für den PC Adobe Digital Editions[10] und für dein Smartphone die App Aldiko Book Reader.[11] Bei E-Book-Readern ist in der Regel eine Adobe-DRM-kompatible Software bereits vorinstalliert. Schließlich musst du die Lese-Software mit deiner Adobe-ID autorisieren. Öffne dazu das installierte Programm und gib die E-Mail-Adresse sowie das persönliche Passwort deiner Adobe-ID an. Nun ist alles vorbereitet um dein erstes E-Book von Onleihe auszuleihen. Das ausgeliehene E-Book darfst du auf maximal 6 Lesegeräte kopieren.

„Weicher“ Kopierschutz

Der „weiche“ Kopierschutz ermöglicht dagegen, das E-Book frei zu nutzen. Der Nutzer kann das Buch auf beliebig viele Lesegeräte kopieren, problemlos in ein passendes Format für das Lesegerät konvertieren oder es auch verschenken. Die Lizenz erlaubt hingegen nur, das E-Book persönlich zu nutzen. Zum Schutz vor Raubkopien wird beim „weichen“ Kopierschutz das Wasserzeichen-DRM eingesetzt. Dabei werden beim E-Book-Kauf persönliche Informationen, wie E-Mail-Adresse oder die Transaktionsnummer an sichtbaren oder unsichtbaren Stellen in das Buch integriert. Wird das E-Book in einer offenen Tauschbörse angeboten, kann der ursprüngliche Käufer mithilfe des digitalen Wasserzeichens eindeutig identifiziert werden. Das Wasserzeichen-DRM ist sozusagen die Visitenkarte, die der Käufer bei einer unerlaubten Kopie gleich mitliefert.

E-Books ohne DRM-Schutz

Es gibt auch E-Book-Shops, die E-Books ohne Adobe-DRM und ohne Wasserzeichen-DRM anbieten. Auch bei solchen Anbietern gelten die Lizenzregelungen. Die Nutzer erwerben lediglich eine persönliche Lizenz, eine Weitergabe an Dritte ist nicht erlaubt. Hier setzen die Verlage gänzlich auf die Redlichkeit der Nutzer, dass sie das E-Book nur so nutzen, wie sie es nach der Lizenz nutzen dürfen.

9 Adobe-Webseite: https://www.adobe.com/de/membership/. Klicke auf den Link „Sie sind noch nicht Mitglied? Adobe-ID erstellen“. Fülle das Eingabeformular aus und folge den Anweisungen auf der Webseite. Die bei Adobe angegebene E-Mail-Adresse bildet die persönliche Adobe-ID.

10 https://www.adobe.com/solutions/ebook/digital-editions/download.html

11 Aldiko Book Reader wird in Google Play angeboten. Webseite des Entwicklers: http://www.aldiko.com/

1.1.3.3 E-Book-Formate

E-Books werden in spezialisierten Formaten veröffentlicht, die jeweils unterschiedliche Lese- und Navigationsfunktionen ermöglichen. Zu den wichtigsten Formaten zählen EPUB, KF8 und PDF. EPUB (Electronic Publication) ist ein offener Standard für E-Books, der von den meisten Lesegeräten unterstützt wird. Das Dateiformat ist ein Fließtext-Format und eignet sich gut für Romane. Das KF8-Format ist ein Dateiformat von Amazon, das nur für Kindle (Hardware) bestimmt ist. PDF von Adobe stellt sicher, dass das Originallayout unverändert bleibt. Für E-Book-Reader oder Smartphones sind PDF-Dateien nur bedingt geeignet, weil ein DIN A4-Dokument auf einem 6-Zoll-Bildschirm nicht lesefreundlich dargestellt werden kann.

Abb. 02: Calibre – E-Book Management

Konvertieren der Dateiformate

Kann dein E-Book-Reader bestimmte Dateiformate nicht lesen, dann konvertiere sie mit dem Programm Calibre[12] für Windows in ein passendes Format. DRM-geschützte E-Books können nicht umgewandelt werden. Wie geht es? Öffne Calibre und importiere dein E-Book über *Bücher hinzufügen* in die Calibre-Bibliothek und wähle das gewünschte Ausgabeformat. Klicke dann auf *Bücher konvertieren*. Abschließend musst du nur das E-Book von deinem PC auf deinen E-Book-Reader übertragen. Mit der App Calibre Companion[13] kannst du die Calibre-Bibliothek auf dem PC mit dem Tablet oder Smartphone synchronisieren. Ohne App geht’s auch. Starte dazu Adobe Digital Editions und verbinde den PC mit dem E-Book-Reader via USB-Kabel und übertrage die konvertierten E-Books.

12 Webseite des Entwicklers: http://calibre-ebook.com. Mit Calibre kannst du E-Books nicht nur in die wichtigsten Formate konvertieren, sondern auch lesen, bearbeiten, Online-Buchshops durchsuchen und mit zahlreichen Lesegeräten synchronisieren. FAQ: http://manual.calibre-ebook.com/faq.html. Dank eines Plug-ins kann Calibre auch den Adobe-DRM-Kopierschutz zu entfernen, sodass E-Books frei genutzt werden können.
13 Calibre Companion wird in Google Play angeboten.

1.1.4 Suche im Internet

Neben den Bibliotheken bietet inzwischen das Internet eine schier unerschöpfliche Quelle an Daten und Informationen. Ohne Assistenz wärst du bei der Suche nach Informationen zu „Passwortmanager für PCs und Smartphones“ in den „unendlichen Weiten“ des Netzes verloren. Diese Informationsarbeit kann man nicht selbst bewältigen, sondern ist auf die Hilfe digitaler Assistenten, wie Suchmaschinen oder Webkataloge, angewiesen. Nutzt du Suchmaschinen, dann überträgst du die Recherchearbeit an Informationsassistenten und musst darauf vertrauen, dass diese tatsächlich die relevanten Informationen für dich beschaffen.

> *„Die Schwierigkeit besteht heute nicht mehr darin, Zugang zu Informationen zu erhalten, sondern sie zu finden.“*
>
> Nando Stöcklin, Bildungswissenschaftler

> *„Wir wollen wie eine perfekte Sekretärin sein, die Ihnen alles abnimmt. Eine perfekte Sekretärin weiß schon ein paar Sekunden früher als Sie selbst, was Sie als Nächstes brauchen. Eine perfekte Sekretärin weist Sie auf Nachrichten hin, die Sie interessieren könnten. Eine perfekte Sekretärin sucht Ihnen ein Restaurant, bevor Sie überhaupt Hunger verspüren. Sie schlägt einen Umweg um den Stau vor, von dem Sie noch gar nichts wissen.“*
>
> Scott B. Huffman, Google-Softwaretechniker

1.1.4.1 Suchmaschinen

Was Suchmaschinen können

Suchmaschinen durchforsten mithilfe von Suchrobotern automatisch Webseiten des Internets. Dabei bewegen sich die Softwareroboter auf einer Webseite von Link zu Link, starten von bekannten und gelangen per Linkverweis zu unbekannten Webseiten. Jede neue oder veränderte Webseite, auf welche die Suchmaschine trifft, wird analysiert und indexiert, d. h. die darin enthaltenen Begriffe werden in einer riesigen Datenbank abgespeichert. Suchmaschinen ermitteln etwa, ob sich die gefundenen Wörter im Text, im Titel oder in der Webadresse befinden und welche Metadaten der Autor hinterlegt hat. Startest du eine Suchanfrage, dann durchsucht die Suchmaschine nicht das Web, sondern ihre Datenbank nach dem eingegebenen Suchbegriff. Von den Suchmaschinenbetreibern geheimgehaltene Algorithmen bestimmen dann, in welcher Reihenfolge die Webseiten aufgelistet werden, die den Suchbegriff enthalten. Aus der Sicht der Nutzer soll eine Suchanfrage dazu führen, dass genau jene Webseiten gefiltert werden, die für ihn relevant sind. Welche Informationen für den Nutzer relevant sein könnten, beruht auf Annahmen. Zu den Google-Annahmen zählt beispielsweise die „Link-Popularität“. Diese besagt, dass solche Dokumente wichtig sein müssen, auf die viele Links im Netz verweisen oder die Nutzer am häufigsten aufrufen.[14]

14 Nach eigenen Angaben von Google ist die Anzahl der Links, die auf eine Webseite verweisen, nur ein Relevanzfaktor unter inzwischen 200: https://www.google.de/intl/de/insidesearch/howsearchworks/algorithms.html

Grenzen und Interessen der Suchmaschinen

Suchmaschinen sind weder allwissend noch unparteilich. Zu den Gründen, warum Suchmaschinen nicht auf alle Informationen und Dokumente im Netz Zugriff haben oder bestimmte Internetseiten bevorzugen, zählen:

- Suchmaschinen durchsuchen nur einen Teil des Internets, nämlich das World Wide Web. Nicht durchsucht werden Dienste wie E-Mail, Chat oder SMS. Suchmaschinen finden auch nicht jede Internetseite. So bleiben ihnen Dokumente, zu denen ein Linkverweis fehlt, verborgen. Auch nicht erfasst werden verschlüsselte Dokumente. Zu Dokumenten, die öffentlich nicht zugänglich sind, zählen beispielsweise Patientendaten der Krankenhäuser oder technische Daten der Forschungsabteilung einer Firma. Unzugänglich sind auch jene Informationen, die erst mit der Suchanfrage an ein Webformular dynamisch erstellt werden. Die Kursentwicklung der Aktie XY in den letzten 3 Monaten wird beispielsweise erst mit der entsprechenden Anfrage durch den Webserver eines Börsen-Dienstes erzeugt. Schließlich verstehen Suchmaschinen (noch) nicht den Inhalt von Bildern, Grafiken, Videos,[15] Audios oder Podcasts. Suchmaschinen benötigen Beschreibungstexte für das Indexieren.
- Suchmaschinen leisten keine Qualitätskontrolle der gefundenen Informationen, der Nutzer muss ihre Qualität selbst überprüfen. Veröffentlicht ein Universitätsverlag ein Buch zum Thema „Sicherheit der SSL-Zertifikate“, wird die Arbeit zuvor einem Peer-Review unterzogen. Die Qualität einer Information messen Suchmaschinen mithilfe der Link-Popularität und übersehen dabei neue, wertvolle Informationen. Die User finden so nur die populären Webseiten. Kritiker der Link-Popularität sprechen von der „Tyrannei der Mehrheit“ oder vom „Matthäus-Effekt“.
- Suchmaschinen machen nicht transparent, wie das Ranking der Suchergebnisse zustande kommt. Kritiker der Google-Suchmaschine werfen beispielsweise dem US-Konzern vor, die Suchergebnisse nicht neutral zu sortieren, sondern systematisch eigene Angebote wie „Google Maps“, „Google Shopping“ sowie die der Geschäftspartner zu bevorzugen.[16] Treffen die Vorwürfe zu, behindert Google den Wettbewerb von Mitbewerbern und schadet den Verbrauchern.[17] Das bedeutet, Nutzer können weder fundiert entscheiden, welche Suchmaschine sie nutzen, noch bei welchem eShop sie einkaufen wollen.
- Webmaster, die mithilfe unlauterer SEO-Techniken versuchen, nicht relevante Webseiten auf die vorderen Plätze der Suchergebnisse zu bringen, untergraben das Relevanzmodell der Suchmaschinen. Eine unlautere

15 Forscher vom Fraunhofer-Institut arbeiten bereits daran, Videos „lesbar“ zu machen: http://www.zeit.de/digital/internet/2013-03/cubrik-video
16 Martin U. Müller u. a. (2012): *Der Türsteher*, in: Der Spiegel 43/2012, S. 86-94.
17 Die EU-Kommission leitete im April 2015 eine kartellrechtliche Untersuchung gegen Google wegen Missbrauchs seiner Marktmacht ein: http://europa.eu/rapid/press-release_IP-15-4780_de.htm?locale=en

SEO-Praxis ist etwa, wenn gezielt eine Linkfarm erstellt wird, um eine hohe Popularität der Webseite vorzutäuschen.

Recherchieren bedeutet für viele Nutzer nur bei Google einen oder mehrere Suchanfragen zu stellen. Obwohl die Suchergebnisse in die Tausende oder gar in die Millionen gehen, sehen sich die Nutzer vielfach nur die ersten zwei Webseiten an. Für alltägliche Suchanliegen reicht Google. Für Recherchen von Journalisten, Strafverteidigern, Studenten oder Wissenschaftlern genügt Google nicht. Sie dürfen sich nicht nur auf den Suchindex und den Bewertungsalgorithmus von Google verlassen.

Bezeichnung	Webadresse	Kurzbeschreibung
Bing	http://www.bing.com	Bing ist eine Suchmaschine von Microsoft, die neben Suchergebnissen auch Tipps von Freunden einbindet.
BASE	http://www.base-search.net	Base (Bielefeld Academic Search Engine) ist eine Open-Access-Suchmaschine, welche weltweit die Suche in überwiegend frei zugänglichen Büchern, Artikeln, Ton- und Videodokumenten ermöglicht.
Google	https://www.google.com	Google ist mit Abstand weltweit die größte Suchmaschine.
Google Books	http://books.google.com	Google Books ist eine Bibliothek digital verfügbarer Bücher. Nutzer können in der Regel das Inhaltsverzeichnis und den Anfang des Buches lesen sowie eine Leseprobe sehen; ein Teil der Bücher kann vollständig online gelesen werden.
Google Scholar	http://scholar.google.com	Google Scholar ist eine Wissenschaftssuchmaschine, die wissenschaftliche Publikationen durchsucht. Sie ist eine wichtige Anlaufstelle für wissenschaftliche Recherchen.
MetaGer	https://metager.de/	MetaGer ist eine Meta-Suchmaschine, die ihre Suchergebnisse aus mehr als drei Dutzend Suchdiensten bezieht. Der Nutzer kann bei jeder Suchanfrage festlegen, welche Suchdienste MetaGer nutzen soll.
Musipedia	http://de.musipedia.org	Musipedia ist eine Suchmaschine, die Musikstücke mithilfe einer virtuellen Klaviatur sowie durch Vorpfeifen identifizieren kann.
NameChk	http://namechk.com	NameChk prüft, ob ein Benutzername, Nickname oder Pseudonym in Communities bereits belegt oder noch frei ist. Der Service lässt sich auch für eine „Online-Ermittlung“ einer Person verwenden.

Bezeichnung	Webadresse	Kurzbeschreibung
Qwant	https://www.qwant.com	Qwant ist eine französische Suchmaschine, die Suchergebnisse in den Kategorien Netz, Nachrichten, soziale Netzwerke und Einkaufen anzeigt.
Startpage	https://startpage.com	Startpage ist eine niederländische Metasuchmaschine, der der Schutz der Privatsphäre der Nutzer „heilig“ ist. Sie speichert weder IP-Adresse noch Suchanfrage. Suchanfragen werden standardmäßig verschlüsselt. Die Trefferseiten können per Proxy anonymisiert aufgerufen werden.
Storify	https://storify.com	Storify ist eine Sortiermaschine, mit der Nutzer Inhalte, wie Tweets, Bilder, Videos oder Webseiten aus den sozialen Netzwerken filtern, chronologisch oder thematisch zu Geschichten bündeln und kommentieren können.
TinEye[18]	https://www.tineye.com	TinEye ist eine umgekehrte Bildsuchmaschine. Nutzer laden das abzugleichende Bild hoch oder geben die Bild-URL ein und die Suchmaschine durchforstet das Netz genau nach diesem Bild.
Yasni	http://www.yasni.de	Yasni ist eine Personensuchmaschine.
Yippy	http://yippy.com	Yippy ist eine Metasuchmaschine, welche die gefundenen Dokumente automatisch nach Themengebieten sortiert, den sogenannten „Clouds“.

Tab. 03: Suchmaschinen

18 Google bietet auch eine Rückwärts-Bildersuche an. So geht’s: Rufe Google auf; im Menü oberhalb der Suchleiste findest du den Menüpunkt *Bilder*. Klicke darauf und innerhalb des Eingabefeldes der Google-Bildersuche auf das Kamera-Symbol. Du kannst nun die URL des gesuchten Bildes eingeben oder das Bild direkt von deinem PC hochladen. Die Suchtreffer zeigen an, auf welchen Webseiten das Bild gehostet wird und ggf. auch die Quellangaben zu Urheber oder Vermarkter des Bildes.

1.1.4.2 Techniken der Suchabfragen

> *„Informationen sind der wertvollste Besitz der Menschheit."*
> James Gleick, Wissenschaftsautor

Bevor wir Techniken der Stichwortsuche vorstellen, muss noch Denkarbeit geleistet werden. Denn die Suchergebnisse hängen mit der Qualität der Suchbegriffe zusammen, die du in die Suchmaschinen eingibst. Zur Vorbereitung von Suchabfragen gehört das Sammeln passender Suchbegriffe zum Thema der Recherche. Passend sind solche Suchbegriffe, welche die relevanten Aspekte eines Themas inhaltlich beschreiben. Um Suchergebnisse zu verbessern, kannst du die gesammelten Suchbegriffe um Oberbegriffe, Unterbegriffe, Synonyme,[19] Abkürzungen oder Übersetzungen in andere Sprachen[20] ergänzen.

Unser Thema lautet „kostenlose Passwortmanager für Windows-PCs und Android-Smartphones". Aus der Themenstellung ergeben sich zwei Unterthemen: „kostenlose Passwortmanager für Windows-PCs" und „kostenlose Passwortmanager für Android-Smartphones". Das erste Unterthema enthält die Teilaspekte „kostenlos", „Passwortmanager" und „Windows". Zu jedem Teilaspekt der Fragestellung schreibst du dir Suchbegriffe auf. Erweitere deine Suchbegriffe durch Synonyme. Den Suchbegriff „kostenlos" kannst du durch „Gratissoftware", „Freeware", „Open-Source-Tool", den Suchbegriff „Passwortgenerator" durch „Passwortverwalter", „Passwortmanager" oder „Password Safe" ergänzen und „Windows" durch Windows-Betriebssystem" ersetzen. In einem zweiten Schritt sind für eine kostenlose Android-App entsprechende Ableitungen vorzunehmen.

Sehen wir uns nun einige Werkzeuge an, die man im Grunde bei jeder Recherche einsetzen kann. Gibst du nur ein einzelnes Stichwort in die Suchmaske der Suchmaschine ein, erhältst du mitunter eine Trefferliste mit 100.000 und mehr Webseiten. Tausende von Webseiten lassen sich aber mit vertretbarem Aufwand inhaltlich nicht auswerten. Mit der richtigen Stichwortsuche kannst du die Trefferliste erheblich verkürzen. Die Suchanfragen sind aber nur dann zielführend, wenn du „webfreundliche" Suchbegriffe verwendest, also Begriffe, die in Webseiten vermutlich enthalten sind. So rät die Google-Seite „Tipps und Tricks für die Suche"[21], nicht: „mein Kopf tut weh", sondern beispielsweise „Kopfschmerzen" zu schreiben.

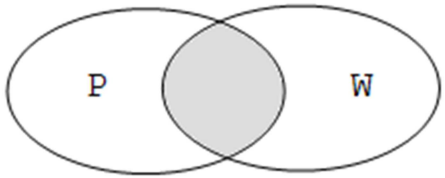
Werkzeuge

Beginnen wir mit den Booleschen Operatoren. Es handelt sich um Verknüpfungen, die dazu dienen, zwei oder mehrere Suchbegriffe logisch miteinander zu verbinden. Die Art und Weise der Verknüpfung wird durch UND, NICHT und ODER geregelt.

---

19 Online-Wörterbücher mit Synonym-Suche: http://www.woerterbuch.info/; https://www.openthesaurus.de/
20 Online-Wörterbücher mit Übersetzungen: https://dict.leo.org/; http://www.dict.cc/
21 https://www.google.com/intl/de/insidesearch/tipstricks/

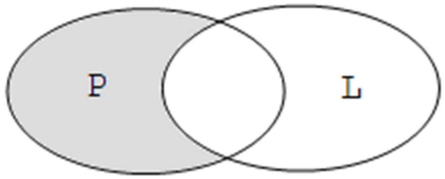
- Der Operator UND (engl. AND) bewirkt, dass zwei Suchbegriffe mit UND verknüpft werden, etwa „Passwortmanager AND Windows“. Der UND-Operator reduziert die Anzahl der Suchergebnisse, es werden nur Dokumente angezeigt, in denen beide Begriffe vorkommen.



P = Passwortmanager
W = Windows

Abb. 03: Suchbegriffe kombinieren: Standard

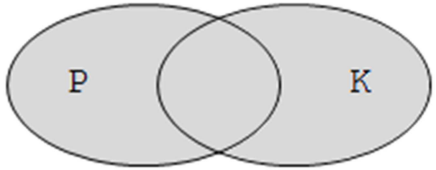
- Der Operator NICHT (engl. NOT) dient dazu, unerwünschte Informationen aus einer Suchanfrage auszuschließen. Die Suche „Passwortmanager NOT Linux“ schließt alle Webseiten aus, welche den Begriff „Linux“ enthalten. Will man bei Google Suchbegriffe ausschließen, muss man ein Minus vor dem Suchbegriff setzen: -Linux.



P = Passwortmanager
L = Linux

Abb. 04: Suchbegriffe kombinieren: NICHT

- Der Operator ODER (engl. OR) erhöht die Anzahl der Suchergebnisse. Bei der Suche nach „Passwortmanager OR Keyverwalter“ werden Dokumente gefunden, welche die Begriffe „Passwortmanager“ oder „Keyverwalter“ oder beide Begriffe enthalten. Die ODER-Verknüpfung hilft insbesondere beim Umgang mit Synonymen und bei verschiedenen Schreibweisen der Suchbegriffe.



P = Passwortmanager
K = Keyverwalter

Abb. 05: Suchbegriffe kombinieren: ODER

Das nächste Werkzeug bildet die Phrasensuche. Setzt man Eigennamen oder zusammengesetzte Begriffe in Anführungszeichen, dann sucht die Suchmaschine exakt nach der ganzen Wortfolge. Sinnvoll sind die Anführungszeichen bei Namen („Bruce Schneier“), Stiftungen („Wikimedia Foundation“), Buchtitel („Filter Bubble. Wie wir im Internet entmündigt werden“) oder Software („KeePass Password Safe“).

Ein drittes Werkzeug sind sog. Joker (Platzhalter). Mit dem Platzhalter Sternchen(*) können beliebig viele Zeichen ersetzt werden. Gibst du als Suchanfrage „Passwort*“ ein, werden Dokumente gefiltert, die mit Passwort anfangen, aber beliebig enden, etwa: Passwortmanager, Passwortkarte, Passwortlänge oder Passwortstärke.

Hierarchische Suche

Das richtige Stichwort für die Suchanfrage ist entscheidend dafür, ob das Suchergebnis relevant und vollständig ist. Bevor du eine Suchanfrage startest, solltest du dir darüber Klarheit verschaffen, über welches Sachgebiet du Informationen suchst. Der beste Weg sich in ein neues Thema einzuarbeiten, ist der der hierarchischen Suche. Stell dir ein Sachgebiet wie eine Pyramide vor. Die gewählten Suchbegriffe sind möglicherweise zu speziell oder zu allgemein.

Suchst du einen kostenlosen Passwortmanager für deinen Windows-PC, dann liefert dir der Suchbegriff *Passwort* nicht nur zu viele und irrelevante Suchergebnisse. In diesem Fall musst du die Suchanfrage enger formulieren. Ist der Suchbegriff zu speziell gewählt, dann ist eine gute Suchstrategie sich von unten nach oben zu arbeiten, etwa statt die Suchbegriffe „Masterpasswort“ oder „Schlüsseldatei“ den Suchbegriff „Passwortmanager“ zu verwenden. Du kannst das Suchergebnis auch verbessern, indem du einen allgemeineren Suchbegriff durch logische Verknüpfung mit speziellen Suchbegriffen verbindest, etwa: „Sichere Passwörter“ AND Passwortmanager AND Freeware AND Windows.

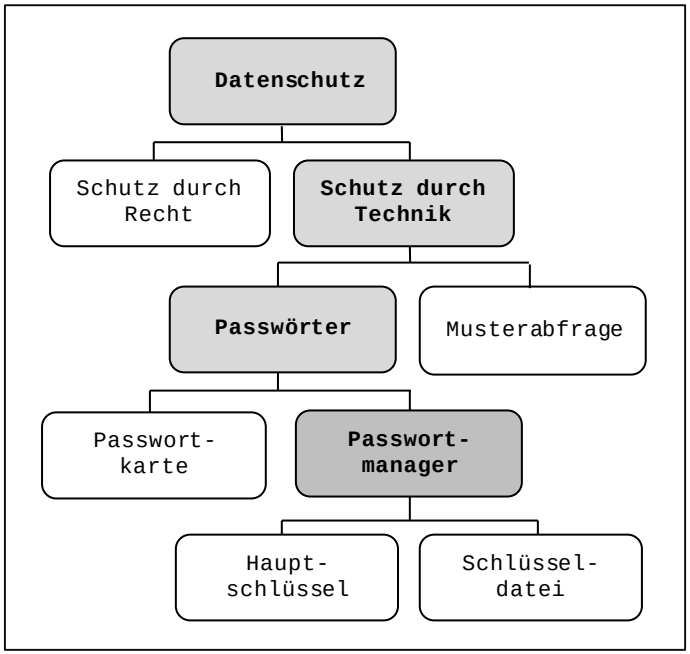


Abb. 06: Hierarchische Suche

Ist das Suchergebnis weiterhin unbefriedigend, dann können auch alternative Suchbegriffe und neue logische Verknüpfungen zwischen den Suchbegriffen weiterhelfen. Bei der Suche nach alternativen Stichworten kannst du auch auf die geleistete Vorarbeit anderer zurückgreifen. Bibliotheken haben ihren Literaturbestand bereits verschlagwortet. Und so kannst du auf die Schlagwortlisten der Bibliotheken zugreifen: Recherchiere in einem Online-Bibliothekskatalog nach der einschlägigen Literatur. Klicke in der Trefferliste auf den Buchtitel, der sich am ehesten mit deiner Suchanfrage deckt. In der Vollanzeige findest du unter den Titeldaten auch die dazu abgelegten Schlagwörter.

Erweiterte Suche

Ein weiteres Suchinstrument die Suchergebnisse zu verfeinern und zu reduzieren bietet die *Erweiterte Suche* von Google. Zur *Erweiterten Suche* gelangst du durch einen Klick auf das Zahnrad rechts oben auf der Google-Startseite. Das Zahnrad wird erst nach einer Suchanfrage eingeblendet. Unter der *Erweiterten Suche* kannst du durch Filter die Ergebnisse gezielt eingrenzen, wie durch Verknüpfungen, Sprache, Dateityp oder Nutzungsrechte. Zu den einzelnen Eingabefeldern gibt es Hilfstexte, sodass du die Suchanfrage passgenau formulieren kannst.

Suche nach bestimmten Dateitypen

Die Suchmaschinen nehmen in ihre Datenbank nicht nur klassische Webseiten im HTML-Format auf, sondern auch eine Vielzahl anderer Formate. Das bedeutet, dass du gezielt nach PDF- oder Office-Dokumenten oder nach MP3-Dateien suchen oder auch bestimmte Arten von Dokumenten aus der Suche ausschließen kannst. Suchst du nach einem bestimmten Dateityp, etwa nach einer .mp3-Datei, dann gib einfach zum Suchbegriff *filetype:mp3* hinzu. Kombinierst du den Dateityp mit weiteren Suchbegriffen, dann findest du schnell die gewünschten Dokumente. Um .mp3-Dateien zum Download von einem bestimmten Interpreten zu finden, gibst du als Suchbegriff dessen Namen, *filetype:mp3* und zusätzlich das Stichwort *Download* ein. Um Konflikte mit dem Urheberrecht zu vermeiden, solltest du die Suche auf CC-Lizenzen einschränken. Die Suchabfrage sieht

dann so aus: *Interpret filetype:mp3 UND Download UND CC-Lizenz*. Bei Google kannst du die Suchanfrage nach bestimmten Dateiformaten auch über die *Erweitere Suche* begrenzen.

Personalisierte Suche

Die personalisierte Suche liefert Suchergebnisse, die genau auf die Interessen und Vorlieben des Nutzers zugeschnitten sind. Die Suchmaschinen protokollieren und werten aus, was Nutzer in der Vergangenheit gesucht, auf welche Links sie geklickt oder welche Inhalte sie weggeklickt haben und passen auf der Grundlage der Nutzerdaten die Reihenfolge der Suchergebnisse an. Bei Google werden Nutzer seit dem Jahr 2012 über alle Google-Dienste hinweg als ein und dieselbe Person identifiziert und behandelt. Das kann dazu führen, dass dieselbe Suchanfrage bei verschiedenen Personen zu unterschiedlichen Suchergebnissen führt. Ein Beispiel: Nutzer, die den „Verschwörungstheorien" zu den Terroranschlägen zum 11. September 2001 glauben, erhalten andere Suchergebnisse als jene Nutzer, die ihre Inhalte mit „kritischem Blick" verfolgen. Anhänger der „Verschwörungstheorien" erhalten zunehmend nur noch Dokumente auf ihre Suchabfragen, die ihr Weltbild bestätigen. Personalisierte Suche kann so dazu führen, dass Nutzer in einem „Filter Bubble" gefangen sind.[22] Die Chance, „Verschwörungstheorien" infrage zu stellen, sinkt, weil Nutzer nicht mehr mit neuen Argumenten und Meinungen konfrontiert werden.

> *„Kreatives Denken und innovative Problemlösungen sind auf Zufälle und Irritationen angewiesen. Irritationen und Zufälle geben dem Denken eine neue, bisher nicht gekannte Richtung. Wenn das Denken irritiert wird, verlässt es seine eingefahrenen Bahnen und findet neue Wege. Erst die Konfrontation mit und die Irritation durch fremde Ideen führen dazu, dass neue Ideen entwickelt werden."*
>
> Volker Boehme-Neßler, Rechtswissenschaftler

Willst du nicht, dass deine Suchabfragen getrackt werden, dann konfiguriere den Browser so, dass nur Sitzungscookies gespeichert werden und säubere den PC regelmäßig von Cookies.[23] Möchtest du nicht, dass Google deine Suchbegriffe trackt und die Suchergebnisse personalisiert, dann logge dich bei Suchanfragen nicht in den Google-Account ein oder verwende Suchmaschinen, die auf Tracking und Personalisierung verzichten.[24]

22 Nach Eli Pariser handelt es sich bei der Filterblase um eine „unsichtbare Echo-Kammer", in der die Nutzer ungefragt und alleine sitzen ohne es zu wissen. Eli Pariser (2012): *Filter Bubble: Wie wir im Internet entmündigt werden,* München, S. 17f; http://www.sueddeutsche.de/digital/eli-pariser-und-die-filter-bubble-ausweitung-der-komfortzone-1.1303419

23 Mit dem Putz-Tool CCleaner können die Cookies bei jedem Systemstart automatisch vom PC gelöscht werden. CCleaner gibt es auch als App für Android: http://www.piriform.com/ccleaner

24 Startpage: https://startpage.com; DuckDuckGo: https://duckduckgo.com/

1.1.4.3 Spezielle Suchdienste und Spezialsuchmaschinen

Google bietet spezielle Suchfilter an, die nur in bestimmten Kategorien, wie Bildern oder Videos suchen. Wer nach einem Buch sucht, kann unter *Google-Bücher-Suche*[25] fündig werden. Du gibst in das Google Bücher-Feld den gewünschten Suchbegriff ein und bekommst alle Bücher angezeigt, deren Inhalt sich mit dem Suchbegriff deckt. Klickst du auf den Buchtitel, werden die bibliografischen Angaben zum Buch und Kritiken zum Buchtitel angezeigt. Ebenso angeführt werden Buchshops, in denen du das Buch kaufen und Bibliotheken, von denen du es ausleihen kannst.

Spezialsuchmaschinen durchsuchen nicht das gesamte Internet, sondern beschränken sich auf ein bestimmtes Themengebiet. Das hat für den Nutzer den Vorteil, dass weniger Informationsschrott im Suchergebnis auftaucht, aber den Nachteil, dass man erst mal die richtige Spezialsuchmaschine finden muss. Nützlich hierfür sind Suchhilfen für Suchmaschinen. Der freie Webkatalog DMOZ (Open Directory Project)[26] ist so etwas wie ein Navi für Suchmaschinen. Das Webverzeichnis bietet Linklisten zu einzelnen Sachgebieten an, die weltweit von freien Mitarbeitern gepflegt werden. Beispielsweise zum Verzeichnis für Spezialsuchmaschinen gelangst du über: *World/Deutsch/Computer/Internet/Suchen/Suchmaschinen/Spezialisierte*.

1.1.5 Lokale Websuche

Eine Vielzahl von Homepages bietet lokale Suchhilfen an, mit deren Hilfe der Nutzer nur die Inhalte dieser einen Homepage durchsuchen kann. Solche Suchhilfen sind für Nutzer besonders hilfreich, wenn sie bei Versandhäusern nach bestimmten Waren suchen, bei Online-Zeitungen eine Archiv-Recherche betreiben, in sozialen Netzwerken nach ehemaligen Schulfreunden, bei Aktionsplattformen nach speziellen Angeboten oder bei Behörden nach einem bestimmten Antragsformular suchen. Als Suchhilfen werden in der Regel die Suche, der Index oder die Sitemap angeboten. Wie die einzelnen Suchhilfen genutzt werden können, findet man vielfach in den Hilfstexten der Anbieter.

Über den Button *Suche* hast du die Möglichkeit, etwa bei einem Online-Buchshop nach Büchern zu suchen, ohne genauere Titelangaben zu haben. Im Suchergebnis findest du dann sämtliche Bücher, die zum Suchbegriff passen. Wie die Suchanfrage bei den einzelnen Anbietern funktioniert, wie eventuell Stichworte kombiniert werden können, wird in der Regel unter *Hilfe* erklärt.

25 https://books.google.de/
26 http://www.dmoz.org

Mithilfe eines Index kannst du die Webseiten nach vorgegeben Stichwörtern durchsuchen; zum Beispiel die Beiträge eines Online-Magazins nach Themen, Jahrgängen oder Autorinnen und Autoren.

Sitemaps zeigen Struktur und Umfang der Homepage an. Über Sitemaps kannst du dir eine Übersicht über eine komplexe Homepage verschaffen und mitunter Themen und Beiträge entdecken, die dir auf den ersten Blick auf der Startseite nicht aufgefallen sind.

1.1.6 Suche in Wikipedia

Die Geschichte der Information ist die Geschichte ihrer Demokratisierung. Im Mittelalter sammelten noch vorwiegend Klöster Informationen und ab dem 17. Jahrhundert stellten öffentliche Bibliotheken Informationen zur Verfügung. Erst mit der massenhaften Verbreitung des PCs in den 1990er Jahren und dem Aufkommen der Online-Enzyklopädien zu Beginn der 2000er Jahre sind immer mehr Menschen an der Produktion von Informationen beteiligt, die potentiell von allen Menschen weltweit genutzt werden können. Die Rede ist deshalb auch von der Informationsgesellschaft.

> *„Stellen Sie sich eine Welt vor, in der jeder Mensch freien Zugang zur Gesamtheit des menschlichen Wissens hat."*
>
> Jimmy Wales, Gründer der Online-Enzyklopädie Wikipedia

> *„Das Besondere an Wikipedia und anderen offenen Systemen ist, dass in ihnen außerhalb herkömmlicher Marktgesetze durch Kooperation Innovationen entstehen, die dank freier Lizenzen allen direkt zur Verfügung stehen."*
>
> Kurt Jansson, Journalist

1.1.6.1 Die Funktionsweise von Wikipedia

Die freie Online-Enzyklopädie Wikipedia wurde im Jahr 2001 vom Internet-Unternehmer Jimmy Wales gegründet. Seit 2003 wird Wikipedia von der gemeinnützigen Stiftung Wikimedia-Foundation getragen. Ziel des Wikipedia-Projektes ist es, eine Enzyklopädie zu werden. Die Beiträge für die Enzyklopädie werden von Freiwilligen verfasst und aktuell gehalten und sind weltweit frei und kostenlos für alle verfügbar. Die wesentlichen Grundsätze der Enzyklopädie sind:

- Gebot der Neutralität: Die Beiträge sollen von einem „neutralen Standpunkt" aus geschrieben werden, d. h. die Autoren sollen „sine ira et studio" (ohne Zorn und Eifer) schreiben. Bei umstrittenen Themen sollen alle relevanten Standpunkte fair zur Sprache kommen. Was in der Öffentlichkeit und der Wissenschaft kontrovers diskutiert wird, sollte auch in Wikipedia entsprechend dargestellt werden.

- Gebot der Transparenz: Inhalte und zentrale Fakten sollen durch Belege untermauert werden. Es sollen nur solche Informationen veröffentlicht werden, die bereits in anderen Medien publiziert wurden. Interessierte können so jederzeit den Wahrheitsgehalt der Beiträge überprüfen. Unter dem Reiter *Versionsgeschichte* kann jeder die Änderung der Inhalte nachvollziehen und unter dem Reiter *Diskussionsseite* verfolgen, wie über Inhalte und Belege diskutiert wird.
- Konzept „Weisheit der Vielen“: Die Beiträge werden gemeinschaftlich verfasst. Die Qualität der Inhalte beruht auf einer selbstorganisierenden Gemeinschaft - ein kollektives Peer-Review. Alle können, ohne besonderen Fachnachweis, Artikel anlegen, ergänzen, aktualisieren oder einen Faktencheck vornehmen, den Stil des Artikels verbessern oder Tippfehler korrigieren. Ein Redaktionsprozess, wie etwa bei Zeitungen, fehlt. Bestand haben jene Inhalte, die von der Community akzeptiert werden. Die Werkstätte der Artikel findet man unter dem Reiter *Bearbeiten*.

Informationen sind[27] …	Klöster	Bibliotheken	Enzyklopädien	Digitale Nachschlagewerke	Online-Enzyklopädien
… verfügbar für ausgewählte Personen	x	x	x	x	x
… verfügbar für alle		x	x	x	x
… 24 h/Tag verfügbar			x	x	x
… aufbereitet für rasche Nutzung			x	x	x
… digital kopier- und durchsuchbar				x	x
… nahezu ortsunabhängig verfügbar					x

Tab. 04: Entwicklung der Informationsbeschaffung seit der Zeit der Klöster bis zur Online-Enzyklopädie

- Grundsatz „freie Inhalte“: Autoren, die Beiträge für Wikipedia verfassen, willigen ein, dass ihre Inhalte unter die freie Lizenz „Creative Commons-Lizenz“ fallen. CC-Lizenz bedeutet, dass die Nutzer die Inhalte privat nutzen, verbreiten, verändern oder auch vermarkten dürfen. Ohne Wikipidia oder die Autoren fragen zu müssen, können Schüler Texte und Fotos für ihren Vortrag verwenden oder Verlage dürfen sämtliche Texte der Wikipedia für eine kostenpflichtige DVD-Ausgabe oder für ein E-Book verwerten.

Die Wikipedia-Artikel haben alle einen ähnlichen Aufbau. Am Anfang steht der Titel, darauf folgt eine Kurzfassung des Inhalts mit Hyperlinks zu ähnlichen Themen. Nach dem Inhaltsverzeichnis folgt ein strukturierter Inhalt mit Hyperlinks zu verwandten Themen. Am Schluss bieten Artikel eine Liste mit weiterführender Literatur sowie Weblinks zum Thema an.

27 Nando Stöcklin (2010): *Wikipedia clever nutzen – in Schule und Beruf*, Zürich, S. 17.

1.1.6.2 Wikipedia richtig nutzen

Für welche Zwecke Wikipedia nutzen?

Wikipedia hat sich als Online-Enzyklopädie etabliert; für Schüler und Studierende ist das Nachschlagewerk unverzichtbar geworden. Seit 2001 sind in englischer Sprache mehr als 4,8 Millionen, in deutscher Sprache über 1,8 Millionen und in italienischer Sprache 1,2 Million Artikel entstanden (Stand: Juli 2015).

Zunächst lässt sich Wikipedia als Suchmaschine nutzen, einfache Fakten lassen sich über Wikipedia schneller finden als über eine Websuche. Ist der Suchbegriff bei einer Websuche nicht präzise genug, erhält man in der Regel eine zu große Trefferliste, die nicht komplett gesichtet und bewertet werden kann. Bei mehrdeutigen Suchbegriffen filtern Suchmaschinen alle Webseiten, die den Suchbegriff enthalten. Gibst du hingegen bei Wikipedia einen mehrdeutigen Begriff wie „Hahn“ ein, dann wirst du als Erstes gefragt, ob mit dem Begriff ein Tier, eine technische oder geografische Bezeichnung, eine Firmenbezeichnung oder ein Personenname gemeint ist. Du wählst dann den passenden Link aus. Überflüssige Informationen fallen so von vornherein weg.

Die Verlässlichkeit der Wikipedia-Artikel ist umstritten. Wikipedia-Kritiker argumentieren, dass es kein Lektorat wie bei Zeitungen oder kein Peer-Review wie bei wissenschaftlichen Publikationen gibt und somit der Wahrheitsgehalt der Information nicht gesichert ist.[28] Andere hingegen fragen sich, ob die Nutzergemeinde die Verlässlichkeit eher fördert, weil viele Augen Inhalte überwachen, korrigieren und aktualisieren. Du kannst die Verlässlichkeit eines Artikels mithilfe dreier Faustregeln fürs Erste bewerten.

- Erstens: Artikel zu prominenten Themen sind verlässlicher als Artikel zu Nischenthemen, weil diese öfters aufgerufen und so Fehler schneller entdeckt werden und weil sich bei umstrittenen Themen die Autoren wechselseitig kontrollieren.
- Zweitens: Artikel mit Qualitätsauszeichnung „lesenswert“ oder „exzellent“ sind verlässlicher einzustufen, weil sie fachlich korrekt und mit Belegen untermauert sind. Solche Auszeichnungen vergeben die Wikipedianer nur nach einer eingehenden vertieften Analyse des Artikels. Lesenswerte Artikel sind rechts vom Artikeltitel mit einem blauen „L“, exzellente Artikel am gleichen Ort mit einem grünen Stern gekennzeichnet.

28 Bereits in der Anfangsphase von Wikipedia haben Untersuchungen ergeben, dass Wikipedia als Informationsquelle etwa so verlässlich ist wie die von klassischen Enzyklopädien. Vgl. Michael Kurzedim (2004): *Wissenswettstreit. Die kostenlose Wikipedia tritt gegen die Marktführer Encarta und Brockhaus an*, in: c’t 2004, Heft 21, S. 132-139. Zu fingierten Wikipedia-Artikeln vgl. https://en.wikipedia.org/wiki/Wikipedia:List_of_hoaxes_on_Wikipedia. In einer Vergleichsuntersuchung aus dem Jahre 2007 zwischen Wikipedia und der Online-Ausgabe des Brockhaus schnitt Wikipedia in den Bereichen Richtigkeit, Vollständigkeit und Aktualität besser ab als der Brockhaus: http://www.stern.de/digital/online/stern-test-wikipedia-schlaegt-brockhaus-604423.html

- Drittens: Rufe die *Versionsgeschichte* und die *Diskussionsseite* zum Artikel auf; so kannst du nachprüfen, welche Textstellen aufgrund welcher Argumente in letzter Zeit geändert wurden.

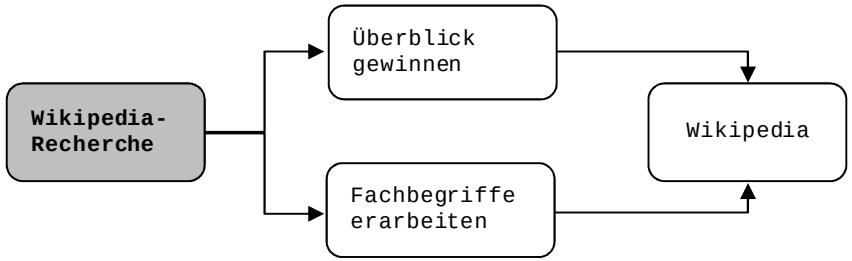


Abb. 07: Wikipedia-Recherche als Einstieg

In jedem Fall kannst du Wikipedia als Einstieg in ein Thema nutzen. Vor einer umfassenden Recherche kannst du dir bei Wikipedia eine Übersicht zu einem Thema verschaffen und dich mit den Fachbegriffen des Sachgebietes vertraut machen. Eine umfassende und vertiefte Recherche kannst du in einem zweiten Schritt vornehmen, in Bibliothekskatalogen, über Suchmaschinen oder über lokale Suchhilfen auf Webseiten. Für die akademische Nutzung ist Wikipedia problematisch, weil die Enzyklopädie nur Informationen wiedergibt, die bereits in anderen Publikationen zu finden sind. Zur wissenschaftlichen Arbeitsweise gehört, dass der Autor seine Informationen aus der Primär- und nicht aus der Sekundärliteratur bezieht.

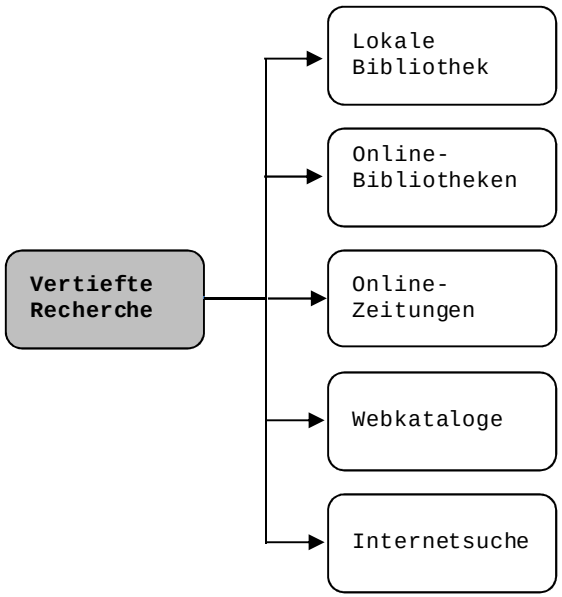


Abb. 08: Vertiefte Recherche

Suchmaschinen können Fotos nur „lesen“, wenn sie von Nutzern markiert oder von Fotografen manuell verschlagwortet wurden. Suchst du beispielsweise nach Urlaubsfotos, um zu wissen, wie die Umgebung um den Reschensee (Italien) aussieht, dann sind Google-Bilder[29] oder die Bilderplattform Flickr[30] nützliche Suchhilfen. Die beiden Bilder-Dienste filtern aber auch Fotos, die mit der Suchanfrage nichts zu tun haben. Wikipedia dagegen liefert präzisere Ergebnisse. Eine Auswahl von Fotos ist im Wikipedia-Artikel selbst eingebunden. Weitere Fotos findest du, wenn du am Ende des Wikipedia-Artikels im Abschnitt *Weblinks* dem Link zu Wikimedia Commons[31] folgst. Die Fotos auf Wikimedia Commons, dem zentralen Medienarchiv von Wikipedia, stehen unter der CC-Lizenz. Die freie Lizenz ermöglicht, dass du die Bilder nach

29 http://images.google.de
30 http://www.flickr.com
31 http://commons.wikimedia.org

Belieben nutzen, kopieren, verändern oder vermarkten kannst.

Wikipedia kannst du auch als Übersetzungsdienst nutzen. Die Online-Enzyklopädie gibt es nämlich in 288 Sprachversionen (Stand: Mai 2015), die untereinander verlinkt sind. Gib probehalber in die Suchmaske der deutschsprachigen Version den Suchbegriff *Share Economy*[32] ein. In der linken Spalte neben dem Artikel unter der Rubrik *in anderen Sprachen* siehst du, mit welchen Sprachversionen der Artikel verlinkt ist. Suchst du Fachbegriffe zur Verschlüsselungstechnik in italienischer Sprache, klickst du auf den Link *Italiano*.[33] Oder gibt es zu einem Suchbegriff keinen deutschsprachigen Artikel, kannst du auch über die englischsprachige Wikipedia[34] zum italienischen Artikel gelangen. Gib hierfür in der englischsprachigen Wikipedia den Suchbegriff ein und rufe dort unter der Rubrik *Languages* den italienischen Artikel auf. Der Vorteil von Wikipedia als Übersetzungsdienst gegenüber online-Wörterbüchern wie dict.leo.org[35] ist, dass die Fachbegriffe in Sätze eingebunden sind und so schnell ihre Bedeutung ermittelt werden kann.

Checkliste Quellenkritik

(in Wikipedia)

Bevor du Informationen aus Wikipedia nutzt, solltest du diese kritisch hinterfragen. Hierzu grundlegende Fragen:

- Handelt es sich beim Artikel um ein prominentes oder um ein wenig bekanntes Thema?
- Ist der Artikel von den Wikipedianern als „lesenswert“ oder „exzellent“ eingestuft worden?
- Wird der Artikel mit externen Quellen untermauert?
- Welche Informationen im Artikel sind unter Wikipedianern umstritten (Diskussionsseite)?
- Sind die Autoren Experten oder Laien zum behandelten Thema?
- Haben die Autoren bereits Publikationen zum behandelten Thema verfasst?
- Wie schätzt der Didaktik-Dienst Wikibu die Verlässlichkeit des Wikipedia-Artikels ein (http://www.wikibu.ch)?

Unter welcher Lizenz stehen Wikipedia-Inhalte?

Die Wikipedia-Inhalte unterliegen nicht dem klassischen Urheberrecht, sondern den Regeln der Creative Commons-Lizenz. Das heißt, jeder kann frei und kostenlos Wikipedia-Inhalte nutzen und verwerten. Rechtliche Vorgaben gibt es nur bei den Zitierregeln. Bei Texten musst du die Quelle, die Autoren, das Datum einer Version sowie die Lizenz anführen, unter der der Artikel steht. Weil die Inhalte in Wikipedia häufig aktualisiert werden und weil jede Änderung unter dem Reiter *Versionsgeschichte* zugänglich ist, sollte beim Zitieren eines Wikipedia-Artikels auch das Datum des Bearbeitungsstands angegeben werden. Der Leser deines Textes sollte im Nachhinein überprüfen können, auf welchen Wikipedia-Inhalt sich das Zitat bezieht. Nutze einfach die Zitierempfehlung von Wikipedia. Rufe den Wikipedia-Artikel, den du zitieren willst. Links unter der Menübox *Werkzeuge* findest du den Link *Seite zitieren*. Klickst du darauf, dann erhältst du unter „Einfache Zitatangabe zum Kopieren“ eine Kopiervorlage für die Quellenangabe.

32 https://de.wikipedia.org/wiki/Share_Economy
33 https://it.wikipedia.org/wiki/Consumo_collaborativo
34 https://en.wikipedia.org
35 http://dict.leo.org/

Bei den Autorenangaben reicht ein Link auf die Versionsgeschichte des Artikels; die einzelnen Autoren, welche den Artikel bearbeitet haben, müssen nicht angeführt werden. Veränderte Texte aus Wikipedia dürfen nur unter derselben Lizenz, also CC-Lizenz, veröffentlicht und verbreitet werden. Fotos, Audios und Videos können von den Autoren unter verschiedenen Lizenzen auf Wikipedia hochgeladen werden. Die jeweilige Lizenz findest du auf der Detailseite der jeweiligen Datei.

1.1.7 Recherche 2.0

Bei der Recherche 2.0 geht es um Inhalte, die Nutzer in kooperativer Weise erstellen. Eine Internetrecherche muss nicht mehr alleine vor dem Bildschirm des PCs durchgeführt werden. Nutzer können sich mit anderen Personen verbinden, die ähnliche Recherchen im Netz durchführen.

Eine erste Suchhilfe bieten Social Bookmarking-Portale. Die Grundidee von Social Bookmarking ist, statt Lesezeichen lokal im Browser auf Social Bookmarking-Portale, wie Google Bookmarks,[36] Diigo[37] oder LinkArena[38] zu speichern. Die Vorteile der Lesezeichen-Gemeinschaften sind, dass Nutzer ihre Lesezeichen nicht nur online verwalten können, sondern von jedem PC, im Internetcafé oder im Büro auf die hinterlegten Lesezeichen zugreifen können, dass sie ihre Lesezeichen mit Schlagwörtern („Tags“) versehen und dass sie die gesammelten Lesezeichen per Mausklick mit anderen Nutzern teilen können. Auf diese Weise profitieren alle, wie bei Wikipedia“, von der „Weisheit der Vielen“. Der Nutzer sieht, wer welche Lesezeichen in seine Sammlung aufgenommen und mit welchen Tags gekennzeichnet hat. Die hinterlegten Lesezeichen lassen sich später anhand von Tags durchforsten. Linksammlungen sind nützlich, wenn man sich einen Überblick über ein Thema verschaffen möchte oder wenn man von Nutzern kommentierte Informationen zu einem Thema sucht.

Eine zweite nützliche Suchhilfe stellt die Plattform Scribd[39] dar, auf die Nutzer selbst Dokumente hochladen oder zur Suche von Dokumenten nutzen können. Die Plattform wird auch als „YouTube für Bücher“ bezeichnet. Nutzer können dort beispielsweise als Filter die Sprache des Dokuments festlegen oder wählen, dass nur kostenlose Dokumente angezeigt werden. Unter „Sammlungen“ werden Dokumente zu einem Thema gelistet, die andere Nutzer zusammengestellt haben.

36 https://www.google.com/bookmarks
37 https://www.diigo.com; Diigo gibt es auch als Android-App auf Google play.
38 http://linkarena.com
39 https://de.scribd.com

1.1.8 Sicher recherchieren

Nutzer, die im Netz nach Informationen suchen, hinterlassen dabei unweigerlich Datenspuren. Solche Datenspuren entstehen bereits bei der Einwahl ins Internet. Für den Zugang zum Netz benötigt der Nutzer eine Zugangsberechtigung, welche der Access-Provider erteilt. Mit der Zugangsberechtigung weiß der Provider, wer der Nutzer ist, weil er dafür seinen Vornamen, Namen, Geburtsort, Geburtstag, das Geschlecht und die Rufnummer preisgeben muss. Ruft er über sein Smartphone eine Webseite auf, protokolliert der Access-Provider die zugewiesene IP-Adresse, Datum und Uhrzeit der Einwahl und die Rufnummer des Nutzers.

Daten entstehen ferner beim einfachen Surfen. Ruft der Nutzer eine Webseite auf, tauschen Browser und Webserver im Hintergrund Informationen aus. Der Webserver protokolliert beispielsweise Informationen zu Browsertyp, Betriebssystem, Fenstergröße, Monitorauflösung, Länderkennung, Spracheinstellung oder Schriftarten. Bereits mit diesen Parametern kann der Webanbieter ein möglichst genaues Profil vom Browser des Nutzers erstellen.[40] Akzeptiert der Nutzer Cookies, ist der PC des Nutzers identifizierbar. Klickt der Surfer eine Werbeanzeige an, wird das gespeichert und ebenso, ob diese zum Kauf des angepriesenen Artikels geführt hat.[41] Eine weitere Trackingtechnologie sind die 1x1-Pixel. Ruft der Nutzer eine Webseite auf, werden diese 1-Pixel-Bildchen ungefragt von Webservern nachgeladen. Setzen Werbetreibende solche Technologien auf einer Vielzahl von Webseiten ein, können sie das Surfverhalten der Nutzer systematisch ausforschen und für personalisierte Angebote nutzen.[42]

Jede Informationsabfrage bei einem Hotel-Portal macht die Interessen des Nutzers transparenter. Jede Recherche hat einen Datenpreis. In der Regel erfahren Nutzer nicht, in welchem Umfang Daten gespeichert und für welche Zwecke sie genutzt werden. Werden die Puzzlestücke, über welche Betreiber der Suchmaschinen, Gewinnspieleanbieter, Versandhändler, App-Anbieter, Cloud-Anbieter und soziale Netzwerke verfügen, verknüpft, entsteht ein virtuelles Personenprofil, das relativ präzise über Interessen, Surf- und Konsumverhalten Auskunft gibt. Für Marketingagenturen ist dieses „Kunden-Genom“[43] die Grundlage für ein erfolgreiches individualisiertes Marketing, etwa welche Reiseangebote oder welche Bücher und Zeitschriften uns an-

40 Die Webseite Panopticlick (https://panopticlick.eff.org/) zeigt dir an, wie einzigartig dein Browser-Fingerabdruck ist. Rufe die Webseite auf und klicke den Button *Test me* an. Je höher der Wert in der Spalte *one in x browsers have this value* ist, um so eher kann der Browser bei einem wiederholten Besuch einer Webseite wiedererkannt werden.

41 Ariane Krol u. a. (2013): *Spione des Marktes. Was Werbung im Internet alles kann,* Le Monde diplomatique Nr. 10130, 14.6.2013, http://www.monde-diplomatique.de/pm/2013/06/14.mondeText.artikel,a0056.idx,22

42 Das Firefox-Add-on Lightbeam (https://www.mozilla.org/de/lightbeam/) zeigt grafisch an, wie dein Surfverhalten im Netz von Datensammlern verfolgt wird. Nach der Installation erscheint in der rechten unteren Ecke des Bildschirms ein Icon. Klickst du darauf, wird ein Tab im Browser geöffnet, in dem du zwischen den drei Lightbeam-Ansichten „Graph“, „Clock“ und „List“ wählen kannst.

43 An einem „360-Grad-Blick“ über Kunden ist beispielsweise die Firma Axciom interessiert; sie führt zu diesem Zweck Offline- und Online-Daten zusammen: http://www.zeit.de/2013/28/acxiom

geboten werden. Die Firma Google beispielsweise verknüpft seit 2012 persönliche Daten, die ein Nutzer bei einem der Google-Dienste hinterlässt, wie bei der Suchmaschine, bei Gmail, YouTube, Google+ oder Android zu einem „Super-Profil“.[44]

Sicher und anonym recherchieren

Willst du unbeobachtet nach Informationen und Dokumenten suchen, dann musst du eine SSL-Suche vornehmen. Bei einer SSL-Suche werden deine Suchanfragen verschlüsselt, sodass weder Firmen noch Behörden deine Suchbegriffe und Suchergebnisse abfangen können. Verschlüsselte Verbindungen erkennst du an der Protokollangabe „https://“ in der Adresszeile und am geschlossenen Schloss. Die Metasuchmaschinen Startpage[45] und DuckduckGo[46] verwenden standardmäßig die Suche per SSL und speichern zudem weder Suchanfragen noch die IP-Adressen der Nutzer. Nutzt du die Google-Suchmaschine, musst du die entsprechenden Webseiten mit SSL-Suche[47] aufrufen, um unbeobachtet recherchieren zu können.

„Eine Gesellschaft, in der das Recht auf Privatsphäre nicht existiert, kann keine freie Gesellschaft sein, da die übrigen liberalen Grundrechte ohne Privatsphäre nur Scheinansprüche sind, die nicht gelebt werden können.“
Maximilian Hotter, Rechtswissenschaftler

Tipp
Lösche von Zeit zu Zeit die gespeicherten Cookies auf deinem PC und blockiere die Schnüffel-Scripts auf Webseiten mithilfe der Firefox-Erweiterung Ghostery. Mit dem Reinigungstool CCleaner kannst du die Surfspuren bei jedem Systemstart auch automatisch entfernen lassen.

Am einfachsten ist, wenn du dir die SSL-Suche deiner bevorzugten Suchmaschine als Startseite anlegst. So geht’s: Nutzt du Firefox als Browser, dann rufe die Webseite auf, die du als Startseite festlegen willst, und kopiere die URL in die Zwischenablage. Gehe über *Extras/Einstellungen* zum Abschnitt *Allgemein* und füge in das Eingabefeld die URL aus der Zwischenablage ein, klicke auf die Schaltfläche *Aktuelle Seite verwenden* und bestätige die neue Startseite mit *OK*. Beim MS Internet Explorer kannst du die entsprechenden Anpassungen unter *Extras/Internetoptionen* im Abschnitt *Allgemein* vornehmen.

Die SSL-Recherche verhindert nur, dass Dritte deine Suchanfragen beobachten können. Der Betreiber der Suchmaschine sieht dagegen weiterhin deine Suchanfragen. Ein anonymes Recherchieren ermöglicht das kos-

44 Google-Managerin Alma Whitten: Wir werden „Sie über alle unsere Dienste hinweg als einen einzigen Nutzer behandeln“. Ziel des übergreifenden Nutzerprofils ist es nach Whitten, ein digitaler Assistent für den Nutzer zu werden: „Wir können Ihnen eine Erinnerung schicken, dass Sie zu einer Verabredung zu spät kommen werden, in Abhängigkeit von Ihrem Aufenthaltsort, Ihrem Kalender und unseren Erkenntnissen über die Verkehrslage.“ Online: http://www.spiegel.de/netzwelt/netzpolitik/persoenliche-daten-google-will-alles-ueber-dich-wissen-a-811221.html. In diesem Fall liegt ein klarer Verstoß gegen das Datenschutzrecht vor, weil eine ausdrückliche Einwilligung des Nutzers zur Verknüpfung der Nutzerinformationen sowie ein Widerspruchsrecht nicht vorgesehen sind.
45 https://startpage.com
46 https://duckduckgo.com/
47 https://www.google.com

tenlose Tor-Browser (Firefox)-Paket,[48] das die Suchanfragen über das verschlüsselte Tor-Netzwerk leitet. Rufe die Webseite des Tor-Projektes auf, klicke unter *Our Projects* auf *Tor Browser*. Unter dem Abschnitt *Download Tor Browser Bundle* findest du die gewünschte Sprache der Programmoberfläche.

1.2 Informationen beurteilen

1.2.1 Recherche, Vertrauen und Skepsis

Recherche und Vertrauen

> *„Kaum etwas von dem, was ich weiß, weiß ich durch eigene Erfahrung, durch eigenes Ausprobieren oder Beobachten."*
>
> Jörg Friedrich, Philosoph

Heute kann jeder, der will, eine eigene Webseite ins Netz stellen. Die angebotenen Informationen können vom Informationsschrott über Spekulationen bis zu wissenschaftlich gesicherten Informationen reichen. Die Suchroboter der Suchmaschinen analysieren und indexieren jede Webseite, unabhängig von der Qualität der bereitgestellten Informationen. Damit stellt sich aber die Frage, ob es im Umfeld des Web 2.0 überhaupt möglich ist, die Zuverlässigkeit der gefundenen Informationen zu beurteilen.

Zunächst eine Bemerkung zur Zuverlässigkeit unserer eigenen Beobachtungen. In der Regel plagen uns keine Selbstzweifel, wenn unseren Überzeugungen eigene Beobachtungen oder Erfahrungen zugrunde liegen.[49] Dass sich aber auch Augenzeugen mitunter irren können, lehren uns Justizirrtümer. Identifiziert ein Augenzeuge den Falschen als Komplizen bei einem Banküberfall, kann das zu einem Fehlurteil führen. Zum Schutz des Angeklagten vor einer falschen Identifizierung sieht das Strafverfahren vor, dass dem Zeugen nicht nur der Beschuldigte, sondern mehrere Personen gleichen Geschlechts, ähnlichen Alters und Aussehens gegenübergestellt werden müssen. Der erfahrene Strafverteidiger wird durch ein Kreuzverhör des Augenzeugen falsche Identifizierungen entlarven. Im Gerichtsprotokoll ist zu lesen „ich bin mir da ganz sicher", aber am Ende stellt sich heraus, dass sich der Augenzeuge geirrt hat.

48 Webseite der Entwickler: https://www.torproject.org/; Anleitung zur Tor-Nutzung: http://www.zeit.de/digital/datenschutz/2013-01/serie-mein-digitaler-schutzschild-tor-browser-bundle

49 Die eigene Beobachtung beruht bereits auf Fertigkeiten, die wir von anderen gelernt haben. Wir können nicht sehen, dass der Akku unseres Smartphones nur noch maximal 4-5 Stunden durchhält, wenn wir die Akkuanzeige nicht verstehen. Der Akkuladezustand springt uns nicht „ins Auge", wenn wir hierfür nicht das Displaysymbol kennen und nicht wissen, dass es auf dem Standardbildschirm rechts oben zu finden ist. Entweder hat uns jemand auf das entsprechende Symbol hingewiesen oder wir haben den Hinweis in der Gebrauchsanleitung gelesen. Strenggenommen haben wir also bereits anderen vertraut, sobald wir etwas mit „eigenen Augen" sehen.

Stammen die Informationen nicht von uns selbst, sondern von anderen Personen, dann stellt sich umso drängender die Frage ihrer Verlässlichkeit. Ohne Informationen von anderen Personen wären wir jedoch in unseren Handlungsmöglichkeiten sehr eingeschränkt. Die meisten Informationen, die wir täglich in der Schule, im Beruf oder im Alltag benötigen, haben wir weder aus eigener Erfahrung noch aus eigener Beobachtung gewonnen. Schüler vertrauen dem Mathematiklehrer, dass er den Rechenweg richtig erklärt; der Kleinanleger glaubt dem Wertpapierberater der Hausbank, dass er sachkundig und unabhängig über die Risiken bestimmter Wertpapiere aufklärt; die Bürger verlassen sich darauf, dass die Eilmeldung des eigenen Radiosenders über den Rücktritt der Regierung richtig ist. Wir vertrauen dem Mathematiklehrer, weil er von der Schule nur eingestellt wird, wenn er eine zertifizierte Fachkompetenz vorweisen kann. Den Informationen des Wertpapierberaters glauben wir, weil er nicht nur die bankeigenen Produkte, sondern auch die der Mitbewerber angeboten hat, und weil das Beratungsprotokoll für ihn keine lästige Formalie ist, sondern sich stets mit dem tatsächlichen Beratungsgespräch deckt. Der Eilmeldung des Radiosenders glauben wir, weil wir wissen, dass die Redaktion nur sorgfältig geprüfte Informationen verbreitet und weil Redakteure für ihre akribischen Recherchen bekannt sind.

Wollen wir überprüfen, ob der Landwirt, der sich als Biobauer ausgibt, tatsächlich nach biologischen Standards wirtschaftet, können wir zu ihm hinfahren und uns vor Ort ein Bild von seiner Arbeitsweise machen. Das funktioniert im Netz nicht. Wer die Person wirklich ist, die gerade mit uns chattet, können wir nicht mit Bestimmtheit sagen. Ist es wirklich der Geschäftspartner oder ist es jemand, der sich dafür ausgibt? Laden wir vom Freeware-Portal tatsächlich das kostenlose Antivirenprogramm herunter oder sind wir gerade dabei uns ein als Antivirenprogramm getarntes Spionagetool einzufangen?

Vertrauen und Skepsis

Die Nutzer können von der Wissensgesellschaft profitieren, wenn sie die Techniken des Recherchierens beherrschen. Für erfolgreiche Recherchen reicht jedoch das eigene Können nicht aus. Finden wir eine Passwort-App für‘s Handy, sind kritische Fragen unumgänglich. Kann man dem Programmierer vertrauen? Hat er die App schlampig programmiert, weist sie Sicherheitslücken auf oder hat sie sogar einen Keylogger mit an Bord, der die abgelegten Passwörter ausspioniert? Laden wir die App von Google Play herunter, dann müssen wir darauf vertrauen, dass der Download technisch funktioniert und dass die App vom Google-Server über das Mobilfunknetz unversehrt auf unser Handy gelangt. Bis wir mithilfe der App das erste Passwort generieren, hat sich eine lange Vertrauenskette gebildet, der wir nicht blind vertrauen sollten.[50]

50 Die Vertrauensbildung im Netz kann nicht von „Angesicht zu Angesicht“ erfolgen. Freunde etwa nehmen „Rücksicht“ auf Interessen und Wünsche ihrer Freunde und unterstützen mit „Wohlwollen“ ihre Lebenspläne. Die Internetnutzer hingegen können nur darauf vertrauen, dass die Personen, die bei Online-Anbietern tätig sind, sich an vertrauenswürdige Regeln und Standards halten oder dass etwa vertrauenswürdige Websiegel für die Seriosität des Anbieters bürgen. Vgl. Martin Hartmann (2011): *Die Praxis des Vertrauens,*

1.2.2 Bewertungskriterien

Für den Nutzer stellt sich somit die Frage, ob es brauchbare Kriterien gibt, um die Zuverlässigkeit der gefundenen Informationen einschätzen zu können. Eine erste Hilfe hierfür bieten formale Kriterien. Welchen Eindruck vermittelt die Webseite? Ist sie gut strukturiert oder unübersichtlich aufgebaut? Strenggenommen ist es nicht zulässig, von der äußeren Erscheinung einer Webseite auf die Qualität der angebotenen Informationen zu schließen – aber sie sollte Anreiz sein, einen zweiten, kritischen Blick auf die Webseite zu werfen. Die nachfolgenden Kriterien sollen Anhaltspunkte liefern, damit du eine Bewertung der Suchergebnisse selbst vornehmen kannst.

Handelt es sich um Werbung?

Suchmaschinen werden in der Regel über Werbung querfinanziert, die in Form von Anzeigen und bezahlten Einträgen eingeblendet wird. Die Betreiber von Suchmaschinen erhalten Geld, wenn der Nutzer den gesponserten Link aufruft und tatsächlich das beworbene Notebook kauft. Die bezahlten Einträge erkennt man vielfach an dem Zusatz „Sponsorenlinks“, „Sponsored Link“, „Partnerlinks“ oder „Anzeige“. Bei Google erscheint Werbung zu Beginn oder neben der Trefferliste. Bei anderen Suchmaschinen ist Werbung aber nicht immer als Werbung gekennzeichnet. Daher sollte man die Ergebnisliste kritisch betrachten, bevor man auf irgendeinen Link klickt.

Ist die Information relevant?

Ist die Quelle wichtig für das Thema? Relevant sind Informationen dann, wenn sie die Fragestellung beantworten und nicht nur einen Randbereich des Themas abdecken. Steht der Suchbegriff im Titel eines Buches oder Dokuments, dann kann die gefundene Information relevant sein. Titel können aber auch irreführend sein: Der Buchtitel „Landschaftspflege“ kann sich mit Maßnahmen zur nachhaltigen Nutzung der natürlichen Ressourcen befassen oder sich mit neuen Enthüllungen zur „politischen Landschaftspflege“ via Spendengelder beschäftigen. Ist das Buch oder das Dokument verschlagwortet, kann sich die Frage der Relevanz schnell klären. Richtet sich das Dokument an Experten oder handelt es sich um die vielfach beklagte Hausarbeit, die per „Copy & Paste“ erstellt wurde? Recherche ist in der Regel ein Prozess. Man hat Vorwissen und eine Idee zu einem Thema, sucht, sichtet, wählt aus, präzisiert daraufhin die Fragestellung, weil man einen ersten Überblick über ein Thema gewonnen hat und wählt neue Suchstrategien.

Berlin, S. 177-182, 283-286. Mehr zum Vertrauen im Internet: Rainer Kuhlen (1999): *Die Konsequenzen von Informationsassistenten. Was bedeutet informationelle Autonomie oder wie kann Vertrauen in elektronische Dienste in offenen Informationsmärkten gesichert werden?* Frankfurt a. M.

Wer ist der Urheber der Information?

> *„Im Internet weiß niemand, dass du ein Hund bist“.*
> The New Yorker 1993

Gibt es Kontaktadressen auf der Webseite? Private Webseiten sollten zumindest Name und E-Mail-Adresse des Inhabers anführen. Gewerbliche Anbieter sollten in jedem Fall Anschrift, Telefon, E-Mail-Adresse und Mehrwertsteuernummer enthalten. Wer der Anbieter einer Information ist, kannst du auch durch eine Whois-Abfrage bei der jeweiligen zentralen Registrierungsstelle für Domains ausforschen. Über eine Domain-Abfrage erhältst du Informationen zum Domaininhaber. So kannst du die Domaininhaber, die in Italien registriert sind, über NIC.it[51] finden und die nicht in Italien registriert sind, beispielsweise über DomainTools.[52]

Sicherheit über die Identität einer Person oder einer Firma liefern TrustCenter. Das TrustCenter stellt ein digitales Zertifikat aus, durch welches die Identität des Web-Anbieters, des Chat- oder E-Mail-Partners bescheinigt wird. Ein solches digitales Zertifikat erkennst du an der Protokollangabe „https://“ in der Adresszeile des Browsers. Solche Zertifikate enthalten u. a. Angaben über den Namen des Web-Anbieters und des TrustCenters. Vertraust du dem digitalen Zertifikat, kannst du auch darauf vertrauen, dass der Kommunikationspartner tatsächlich der ist, der er vorgibt zu sein.

Ist der Autor Experte auf dem Gebiet? Ist er Inhaber eines Lehrstuhls an einer Universität? Spielt der Autor mit offenen Karten, benutzt er exakte Daten, sind sie überprüfbar und macht er Zitate kenntlich? In überregionalen Bibliothekskatalogen, wie in WorldCat,[53] kannst du nach dem Namen suchen und herausfinden, was der Autor sonst noch zum Thema publiziert hat. Gibt es Kurzbiografien zum Autor?

Welche Interessen verfolgt der Anbieter?

Will der Verfasser objektiv informieren, belegt er seine Aussagen und macht seine Arbeitsweise transparent, sodass die angebotenen Informationen nachvollziehbar und überprüfbar sind. Vertrauenswürdige Quellen führen stets das WER, WO und WANN an. Verfolgt der Anbieter kommerzielle Interessen, sind Werbebanner auf der Seite zu finden? Will der Anbieter etwas verkaufen? Enthält die Webseite Fakten oder Meinungen? Handelt es sich um bezahlte Einträge, sagt uns der Hausverstand, dass wir von solchen Webseiten keine ausgewogenen, fundierten Informationen erwarten dürfen.

51 http://www.nic.it/web-whois/index.jsf
52 http://whois.domaintools.com/
53 http://www.worldcat.org

Ist die Information aktuell?

Wie aktuell ist die veröffentlichte Information? Wird das Webangebot regelmäßig aktualisiert? Werden regelmäßig neue Erkenntnisse in Wissenschaft und Technik oder neue gesetzliche Regelungen in die angebotenen Informationen eingearbeitet? Eine sichere Verschlüsselungstechnik der 1970er Jahre kann 40 Jahre später nicht mehr als sicher gelten.[54] Die Aktualität von PDF-Dokumenten kann beispielsweise in den Dokumenteigenschaften überprüft werden. Dabei ist zu beachten, dass das Erstellungs- bzw. das Änderungsdatum sich nicht zwingend auf den Zeitpunkt der inhaltlichen Erstellung des Dokuments beziehen muss, sondern lediglich auf den Zeitpunkt der Konvertierung eines Word-Dokuments ins PDF-Format. Die Angaben der Suchmaschinen zur Aktualität von Informationen sind nicht zuverlässig, weil es sich lediglich um das Datum der letzten Indexierung handeln kann. Irrtümlicherweise kann so aus einer überholten eine tagesaktuelle Information werden (vgl. Kurssturz bei United Airlines).[55]

Kurssturz bei United Airlines

„Letzte Woche (September 2008) *vermeldete der Newsservice ‚Google News' den Konkurs von United Airlines – dass die Meldung schon sechs Jahre alt war, wusste zu diesem Zeitpunkt niemand, zumindest nicht die Chicago Tribune.*

Als Reaktion auf diese Konkursmeldung veröffentlichte die Onlineausgabe der Tageszeitung Sun Sentinel einen Artikel – mit verheerenden Auswirkungen. Die Aktie der United Airlines fiel innerhalb von 12 Minuten um 75 Prozent von 12 auf 4,05 US-Dollar, mehr als eine Milliarde Dollar (!) wurde vernichtet. Und das alles wegen einer Falschmeldung. Denn der Airlinebetreiber hatte keineswegs Konkurs angemeldet. Die Meldung von vor sechs Jahren wurde versehentlich von einem Google-Computerprogramm als neu ausgegeben."

Ist die Webseite vernetzt?

Nutze auch die sogenannte Rückwärtssuche. Dabei kannst du ermitteln, wie stark die fragliche Information vernetzt ist und wie andere Personen diese Information bewerten. So geht's: link:URL der Webseite (z. B. die Suchanfrage link:keepass.info) und du bekommst alle Webseiten aufgelistet, die mit der eingegebenen Webseite verlinkt sind. Geht der Link von einer vertrauenswürdigen Webseite aus, ist das ein Indiz, dass die verlinkte Information auch vertrauenswürdig ist. Recherchiere zudem: Wird die Information von Fachkollegen zitiert, akzeptiert oder kritisiert? Gibt es zur gefundenen Publikation gute Rezensionen in Fachzeitschriften, Pressestimmen oder auch sachkundige Leserkommentare? Sichert eine aktive Nutzergemeinde, wie beispielsweise jene bei der Online-Enzyklopädie Wikipedia, durch gemeinschaftliche Kontrollen und Korrekturen die Verlässlichkeit der Informationen? Findet man zu Produkteigenschaften nur Kundenbewertungen bei Amazon oder auch Tests von Verbraucherzentralen? „Vernetztes Vertrauen" im Verbund mit geschulter Skepsis kann Nutzern helfen, Suchergebnisse richtig zu bewerten.

54 ZEIT online berichtet, dass Millionen SIM-Karten veraltete Verschlüsselungsstandards nutzen und deshalb per SMS gehackt werden können: http://www.zeit.de/digital/mobil/2013-07/sim-karte-hack-nohl

55 Anna Friedrich (2008): *Google News verursacht Kurssturz bei United Airlines,* Themenblog, 19.09.2008, http://themenblog.de/2008/09/19/google-news-verursacht-kurssturz-bei-united-airlines/

Ist die Information vollständig?

Die Suchmaschinen zeigen in ihren Trefferlisten zuweilen nur einen Ausschnitt aus dem Gesamtangebot einer Webseite an, Leseproben eines Buches oder nur eine Unterseite einer Homepage. Um eine Information richtig beurteilen zu können, muss man manchmal das vollständige Webangebot kennen. Einen Überblick über das Gesamtangebot erhält man, indem man die Internetadresse von rechts bis zum ersten Slash (/)kürzt oder indem man die Startseite aufruft.[56]

1.3 Informationen festhalten

Suchergebnisse, seien es Links, Artikel oder Bücher, sollten in irgendeiner Form festgehalten werden, damit du später auf sie schnell zugreifen kannst. Denn es ist sehr ärger lich und zeitaufwändig, verloren gegangene Informationen wieder zu beschaffen. Wie man am besten Suchergebnisse festhält, hängt davon ab, für welche Zwecke Gefundenes später genutzt werden soll. Sollen nur Suchergebnisse zu Jugendherbergen, die für einen Wochenendausflug in die engere Wahl kommen, gesichert werden oder will man den Überblick über die Fachliteratur einer akademischen Abschlussarbeit behalten und entsprechend dokumentieren? Im ersten Fall reicht es aus, die betreffenden Webseiten einfach als Lesezeichen im Browser zu speichern, auszudrucken oder als PDF-Dokument[57] abzuspeichern.

Literatur lokal festhalten

Literatur für eine größere Arbeit sollte von Beginn an richtig festgehalten werden. Handelt es sich lediglich um fünf Fachbücher und 30 Fachartikel, die du für deine Arbeit voraussichtlich nutzen willst, kannst du die bibliographischen Angaben auch in Word oder Excel speichern. Für größere Arbeiten kannst du die klassischen Karteikarten[58] verwenden. Gleichzeitig musst du beim Lesen der Originalquelle die relevanten Textstellen markieren oder mit selbstklebenden Zetteln spicken, damit du die Infos auf der Karteikarte im Originaltext wieder findest. Willst du auch unterwegs auf deine Literatursammlung zugreifen können, benötigst du einen webbasierten Dienst.

56 http://www.monde-diplomatique.de/pm/2013/02/08.mondeText.artikel,a0010.idx,0; http://http://www.monde-diplomatique.de/

57 So geht’s: Installiere zunächst das PDF-Tool PDFCreator (http://de.pdfforge.org/). Mit seiner Hilfe kannst du aus beliebigen Programmen heraus mit der Druck-Funktion ein PDF-Dokument erstellen.

58 Zu den Grundsätzen für Karteikarten zählen: eigene Karteikarte für jede Informationsquelle, also Buch, Fachartikel, Webseite, Podcast; fortlaufende Nummerierung der Karteikarten; jede Karteikarte enthält oben Angaben zum Autor, Titel und Herkunftsort und in der unteren Hälfte Kurzinfos, in welchem Kapitel oder Abschnitt das Gelesene in der eigenen Arbeit angeführt werden soll.

Links im Web festhalten

Speicherst du die Links im Web, schlägst du zwei Fliegen mit einem Schlag. Du kannst die Lesezeichen unabhängig von deinem PC verwalten – im Büro, im Internetcafé, bei Freunden oder auf deinem Smartphone – und gleichzeitig die Social Bookmarking-Dienste nutzen.

Eine einfache Lösung stellt Google Bookmarks[59] dar. Bei Google Bookmarks gibt es im Unterschied zum Browser keine Ordner, sondern alles läuft über Schlagworte, den sogenannten Tags. Jeder Link lässt sich mit Schlagwörtern, Google nennt sie Labels, und Beschreibungen versehen. Tags haben den Vorteil, Mehrfachzuordnungen von Lesezeichen vornehmen zu können. Klickst du einen Tag an, werden alle Lesezeichen angezeigt, die du mit diesem Tag gespeichert hast. Nutzer von Google-Chrome können die Lesezeichen-Erweiterung „Bookmark Manager“ installieren, damit Lesezeichen anlegen, verwalten und mit anderen Nutzern, etwa einem Projekt-Team, teilen.

Reicht ein einfacher Dienst wie Google Bookmarks nicht aus, dann kann ein versierterer Dienst wie Diigo[60] eine Alternative sein. Diigo bietet neben der Online-Speicherung von Bookarmks seinen Nutzern Kommunikations- und Kooperationsmöglichkeiten an. Interessante Webseiten können kommentiert, mit anderen Nutzern geteilt und gemeinsam bearbeitet werden. Kombiniert man Tags, lassen sich die gewünschten Informationen bequem filtern. Diigo bietet seinen Nutzern auch die Möglichkeit, ausführliche Profile anzulegen.[61] So können andere Nutzer sehen, mit welchen Themen (Tagcloud) sich Nutzer mit welcher Beharrlichkeit interessieren. Diigo ist insbesondere für Studierende ein mächtiges Werkzeug. Es ermöglicht Kommilitonen, Quellen für ein gemeinsames Referat zu sammeln und sich über die Suchresultate online auszutauschen.

Literatur festhalten

Bei kleineren Literaturrecherchen in Bibliothekskatalogen kannst du die gefundene Literaturliste ausdrucken oder lokal abspeichern. Bibliothekskataloge verfügen in der Regel über Speicheroptionen. Ist man im Studium oder im Beruf an umfangreichen Projekten beteiligt, dann reicht ein einfaches Festhalten der gefundenen Literatur nicht mehr aus. Literaturverwaltungsprogramme schaffen hier Abhilfe. Mit ihnen kann man ohne großen Aufwand Literatur sortieren, einordnen und effizient verwalten.

59 https://www.google.com/bookmarks; damit du den Google-Dienst nutzen kannst, benötigst du ein Google-Konto.
60 https://www.diigo.com/
61 Ein Tutorial zur Nutzung von Diigo: Wolfgang Schumann (2010): *Internetrecherche und Wissensmanagement. Suchresultate festhalten mit Diigo,* http://bit.ly/Xy6dAr

Ein einfach zu bedienendes Programm mit zahlreichen Funktionen ist Zotero.[62] Das Programm kannst du herunterladen und auf dem Computer installieren oder als Erweiterung (Add-on) in den Browser Firefox[63] integrieren. Wir wählen das Firefox-Add-on Zotero.[64] Das Programm ist in drei Spalten aufgebaut. In der linken Spalte findest du eine Übersicht über die Bibliothek und die darin angelegten „Sammlungen“; in der mittleren Spalte sind die halte einer speziellen Sammlung abgelegt; in der rechten Spalte werden die bibliographischen Angaben eines ausgewählten Eintrages angezeigt und können bei Bedarf editiert werden. Die einzelnen Einträge kannst du mit eigenen Notizen ergänzen und mit Tags versehen. Tags sind in großen Literatursammlungen sinnvoll, da sie dir ermöglichen schnell Literatur zu bestimmten Themen in Zotero zu finden.

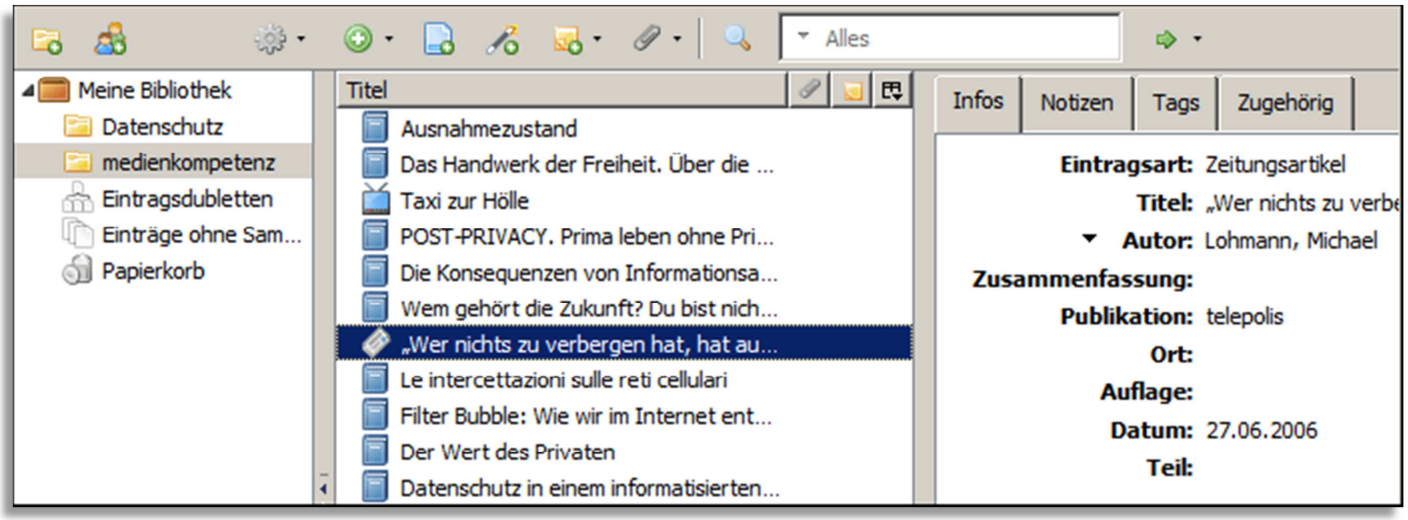


Abb. 09: Literaturverwaltungsprogramm Zotero

Wie kann man neue Medien der Bibliothek hinzufügen? Erstens, es gibt die manuelle Variante. Klicke oberhalb der mittleren Spalte auf das Plus-Symbol, dann kann ein Medium komplett neu erfasst werden. In der rechten Spalte erscheint ein leeres Formular, mit den für den gewählten Medientyp verknüpften Datenfeldern. Zweitens besteht die automatische Variante. Das Tool erkennt auf vielen Webseiten die bibliografischen Angaben von Büchern. Findet Zotero entsprechende Daten, erscheint in der Adresszeile des Firefox ein Buchsymbol. Mit einem Klick darauf werden die Daten in die Zotero-Bibliothek importiert. Zotero erkennt auch Listen mit Publikationen. Ist das der Fall, erscheint in der Adresszeile des Browsers ein Ordnersymbol. Klickst du darauf, poppt ein Dialogfenster auf, indem du die gewünschten Titel auswählen und

62 https://www.zotero.org; Zotero ist eine Open-Source-Software, die vom Center for History and New Media der George Mason University entwickelt wird: http://chnm.gmu.edu/zotero/
63 Ist Firefox auf deinem PC nicht vorhanden, musst du das Open-Source-Tool zuvor installieren: https://www.mozilla.org/en-US/firefox/all/
64 https://www.zotero.org/download/; Add-ons gibt es auch für die Browser Chrome und Safari.

mit *OK* der Bibliothek hinzufügen kannst. Einträge lassen sich auch per „Identifier“ einer „Sammlung“ hinzufügen. Mit „Identifier“ genügt schon das Eintippen einer ISBN-Nummer und Zotero holt sich die bibliographischen Informationen aus dem Netz.

Willst du von überall auf deine Bibliotheks-Daten zugreifen, musst du dich bei Zotero[65] registrieren. Hast du die Daten auf den Zotero-Server hochgeladen, können sie auch automatisch synchronisiert werden. Öffne hierfür die Zotero-Einstellungen über das Zahnrad-Icon, gib unter dem Reiter *Sync* Benutzername und Passwort ein und setze ein Häkchen vor *Automatisch synchronisieren*. Zotero ist auch ein Web 2.0-Werkzeug. Die Server-Option ermöglicht dir „Gruppen“-Bibliotheken zu bilden, sie anderen zur Verfügung zu stellen und gemeinsam zu nutzen.[66]

1.4 Auf dem Laufenden bleiben

Auf dem Laufenden zu bleiben stellt im Studium oder bei manchen Berufen wie IT-Sicherheitsexperten oder Journalisten eine zentrale Voraussetzung dar. Es reicht hier nicht, sich einmal ein umfassendes Bild von der Literatur zu einem Thema zu verschaffen. Regelmäßig Informationen und Literatur zu aktualisieren, wäre zeitaufwändig. Im Wesentlichen gibt es zwei Wege, um am Laufenden zu bleiben: mithilfe von digitalen Assistenten oder mit Hilfe von Menschen.

RSS-Feeds abonnieren

RSS-Feeds zählen zu den digitalen Assistenten. RSS umschreibt einen Service von Webseiten, der es Nutzern ermöglicht einen RSS-Feed zu abonnieren. Der Nutzer muss dann nicht mehr die bevorzugten Webseiten aufsuchen, um zu sehen, ob neue Inhalte veröffentlicht wurden. Der RSS-Feed informiert nämlich automatisch über Veränderungen zur abonnierten Webseite. Die RSS-Feeds können über die Lesezeichen des Browsers oder per webbasierten Feed-Reader angezeigt und verwaltet werden.

Stößt du bei deiner Internetrecherche auf interessante Webseiten, die einen RSS-Feed[67] zur Verfügung stellen, dann kannst du diesen direkt aus dem Browser abonnieren. Um Beiträge zu abonnieren, musst du das RSS-Symbol suchen. Mit einem Klick auf das RSS-Symbol klappt eine Liste auf, in der alle verfügbaren Feeds angezeigt werden. Wähle die RSS-Feeds aus, die du abonnieren möchtest. Im Firefox-Browser kannst du

65 https://www.zotero.org/user/register/
66 Eine umfassende Hilfe zu Zotero findest du online unter: https://www.zotero.org/support/
67 RSS-Feeds werden in der Regel als orangefarbiges Symbol angezeigt, manchmal auch als Textlink („RSS“, „Feed“).

die Feeds als „Dynamische Lesezeichen“ zusammen mit den anderen Lesezeichen verwalten. Klappst du die Feeds auf, dann werden die Überschriften der Einträge angezeigt. Ein Klick auf die Überschrift führt dich direkt zur Webseite, die den Artikel bereitstellt.

Mehr Funktionen bietet die Firefox-Erweiterung Sage.[68] Nach der Installation und dem Neustart des Browsers wählst du *Ansicht/Sidebar/Sage* aus oder klickst auf das Sage-Symbol in der Symbolleiste und rufst die Webseite auf, von der du Feeds abonnieren möchtest. Klicke auf das Lupen-Symbol, dann startet Sage die Suche nach Feeds, die auf der Webseite angeboten werden. Markiere die gewünschten Feeds und drücke auf *Nachrichtenkanal hinzufügen*. In einer Sidebar wird ein Überblick über die abonnierten Feeds und deren Überschriften angezeigt und im Hauptfenster die Überschriften mit Nachrichtentext. Mit einem Klick auf die Überschrift gelangst du zur Vollversion des Artikels.

Abschließend noch einen Blick auf die webbasierten RSS-Reader. Sie haben den Vorteil, dass Nutzer auch von ihren Smartphones oder Tablets aus RSS-Feeds nutzen und verwalten können. The Old Reader[69] gilt als Nachfolger des inzwischen eingestellten Google Readers. Mit The Old Reader lassen sich Feeds mit anderen Nutzern teilen, kommentieren und taggen. Eine Suchfunktion ermöglicht beispielsweise die Titelzeilen der abonnierten Feeds zu durchsuchen. The Old Reader kann auch mobil über Apps für Android, iOS oder Windows Phone genutzt werden.[70]

„Persönliche Lernnetzwerke“

Der zweite Weg auf dem Laufenden zu bleiben geht mit Hilfe von Menschen. Nutzer, die in Sozialen Netzwerken registriert sind, können Literatur- und Informationsanfragen an die Community stellen. Auf Web 2.0 Plattformen wie Facebook können auch thematische Gruppen gegründet werden, in denen Interessensgebiete geteilt werden, Literatur zu einem Thema gesammelt und kommentiert wird. Über Twitter,[71] dem Kurznachrichten-Dienst, können Teamkollegen oder Kommilitonen kurze Fragen stellen, einen Link zu einem lesenswerten Artikel versenden oder auch Tweets von interessanten Personen verfolgen. Mit dem Office-Paket Google Docs können beispielsweise Dokumente in der Google Drive-Cloud erstellt, daran gemeinsam gearbeitet und über die App Google Drive mobil darauf zugriffen werden.[72]

Menschen, die auf Wissensgebieten Informationen teilen, tauschen und diskutieren, bilden „persönliche Lernnetzwerke“ (Personal Learning Network). Lernnetzwerke entstehen nicht per Klick, sondern benötigen

68 https://addons.mozilla.org/de/firefox/addon/sage/
69 https://theoldreader.com/
70 https://theoldreader.com/pages/apps
71 https://twitter.com/
72 Damit du Google Docs nutzen kannst, benötigst du ein Google-Konto.

Zeit, setzen ein „Netzkultur“ voraus und leben von der Erfahrung, dass Wissen sich vermehrt, wenn man es mit anderen teilt. Handelt es sich bei den persönlichen Lernnetzwerken um „selbstorganisierende“ Netze? Sollen „persönliche Lernnetzwerke“ in Schulen etabliert werden, müssen die Lehrer verstehen wie sie funktionieren, wissen wie sie für den Unterricht genutzt werden können und überzeugt sein, dass sie das Lernen unterstützen können. Gefragt sind Mentoren, Workshops oder Leitfäden,[73] die deutlich machen, „worauf es ankommt“, um Blogs, Wikis, Lesezeichen-Gemeinschaften oder soziale Netzwerke fürs Lernen sinnvoll nutzen zu können.

73 EU-Projekt über „persönliche Lernnetze“ für Sprachlehrer (aPLaNet): http://www.aplanet-project.eu/; aPlanet Handbuch für Lehrer: http://www.aplanet-project.eu/Resources/Methodology%20DE/Teacher%20Guide_DE.pdf

1.5 Arbeitsaufträge

1. Das Wachstum der Medienindustrie hängt auch vom Konsumismus der Nutzer ab, also von ihrem Interesse, stets die neueste Soft- und Hardware haben zu müssen. Bildet drei Gruppen und bearbeitet Fragen zur kritischen und überlegten Mediennutzung.

   Gruppe A: Sie untersucht den Nutzen von Software auf PC oder Smartphones.

   a) Wie hat sich der Funktionsumfang der Microsoft Office-Pakete von Office 2007, Office 2010 bis zu Office 2013 entwickelt?
   b) Welche Alternativen gibt es zu Microsoft Office?
   c) Welche Programme haben die Schüler auf ihrem PC oder Smartphone, die sie niemals nutzen?
   d) Wie viel Geld hat jeder Schüler in den letzten 5 Jahren für Software ausgegeben?
   e) Erstellt eine Liste kostenloser Apps für den Schüleralltag. Begründet eure Wahl.

   Gruppe B: Sie analysiert den Nutzen von neuer Hardware am Beispiel von Smartphones.

   a) Recherchiert, wodurch sich die beiden letzten Versionen der Apple iPhone voneinander unterscheiden.
   b) Zeigt auf, inwiefern Apple das Handy-Design revolutioniert hat.
   c) Untersucht, wodurch sich das Geschäftsmodell der Android-Smartphones von dem der Apple-Smartphones unterscheidet.

   Gruppe C: Sie beschäftigt sich mit den Bestimmungsgründen des Konsumismus im Allgemeinen.

   a) Was versteht man unter Konsumismus?
   b) Welche Faktoren bestimmen den Konsumismus?
   c) Wie kann man sich vor den Verführungen des Konsumismus im Bereich Software, Notebooks und Smartphones wirksam schützen?

2. Handys sind inzwischen auch während des Unterrichts präsent. Erstellt Regeln für die Nutzung der Handys an eurer Schule. Wie soll bei Verstößen der Handyregeln vorgegangen werden? Stellt die erarbeiteten Regeln in der Klasse zur Diskussion.

3. Recherchiert, wie groß der weltweite Absatz und Marktanteil der Mobilfunkhersteller ist; insbesondere der von Android- und iOS-Smartphones. Erstellt hierzu ein Balkendiagramm.

4. Im Internet herrscht eine Gratiskultur. Digitalisierte Mediengüter wie Texte, Fotos, Songs, Videos und Spiele gibt es vielfach gratis. Untersucht, wer und aus welchen Beweggründen Wikipedia, Facebook und die Musik-Community-Seite ccMixter finanziert.

5. Bildet eine Gruppe von drei Personen zum Thema „Wettbewerbsregeln für Software“.

   a) Stellt fest, wer von der Klasse nur die vorinstallierten Programme auf dem PC oder Smartphone nutzt. Visualisiert die Ergebnisse in Form eines Balkendiagramms.
   b) Erstellt Wettbewerbsregeln für Browser. Sollten die Betriebssysteme ohne vorinstallierte Browser, wie Internet Explorer, ausgeliefert werden oder sollte der Nutzer „eine Auswahl“ erhalten?
   c) Recherchiert, wie die EU-Kommission gegen Machtmissbrauch bei vorinstallierten Browsern vorgeht und wie sie sich einen fairen Wettbewerb unter Browser-Anbietern vorstellt.

6. Wie sollten sich die Global Player des Internets, wie Apple, Facebook, Amazon, Google oder Finanzdienstleister gegenüber politisch brisanten Online-Inhalten verhalten? Per AGB (Allgemeine Geschäftsbedingungen) eine eigene Hausordnung festlegen? Sich an die Strafgesetze des jeweiligen Landes halten? Dem politischen Druck der jeweiligen Regierung nachgeben? Rechtskräftige Urteile eines fairen Gerichtsverfahrens abwarten?

   a) Sollten beim Versandhaus Amazon auch Bücher angeboten werden, die strafrechtlich ausdrücklich verboten sind, oder sollte Amazon das Recht haben, Verlage und Buchhändler nur solche Bücher einstellen zu lassen, die zur eigenen „Hausphilosophie“ passen?
   b) Julian Assange, Gründer der Enthüllungsplattform WikiLeaks, sammelte u. a. über die Bezahlfirma Paypal Spendengelder für WikiLeaks. Im Jahre 2010 lösten Paypal und Finanzdienstleister ohne rechtskräftiges Gerichtsurteil WikiLeaks-Konten auf und Internet-Hostingfirmen verbannten WikiLeaks von ihren Servern. Kritiker warfen Paypal und den Finanzdienstleistern vor, sich als „Hilfssheriffs der Regierungen“ verhalten zu haben. Sucht im Internet nach Zeitungsartikeln zur umstrittenen Vorgangsweise und bewertet die kontroverse Sachlage.

7. Die Rolle des Konsumenten hat sich in den letzten Jahren verändert. Verbraucher interessieren sich für die ökologischen und sozialen Standards der Zulieferer von Hardwareherstellern.[74]

   a) Recherchiert, ob die Firma Apple in ihrem Smartphone-Sortiment Angebote für den „moralischen Verbraucher“ hat.
   b) Recherchiert, ob die Firma Apple Einfluss auf die Zulieferer nimmt, ihre Produktionsmethoden sozialen und ökologischen Standards anzupassen.

74 Das niederländische Start-Up *Fairphone* will Smartphones unter zumindest teilweise fairen Bedingungen herstellen: http://www.fairphone.com/; Überblick zum Fair-Konzept: http://www.tagesspiegel.de/medien/fair-gehandelte-elektro-produkte-surfen-mit-gutem-gewissen/8588752.html; http://www.tagesspiegel.de/wirtschaft/fairphone-ein-gadget-fuer-das-gute-gewissen/8869280.html; http://www.zeit.de/2013/43/fairphone

c) Erstellt eine Checkliste für nachhaltigen und fairen Konsum für Smartphones.
d) Welche Gütezeichen für Smartphones gibt es und welche Eigenschaften verbürgen sie?
d) Überprüft in eurer Klasse, wie groß die Bereitschaft wäre, etwa für Smartphones mit einem CO2-Label 25 Prozent mehr Geld auszugeben.

8. Macht in eurer Schulklasse eine Erhebung über die Mediennutzung am Tag davor und visualisiert die Ergebnisse in Form von Diagrammen.
   a) Welche Medien habt ihr genutzt?
   b) Wie lange habt ihr die Medien genutzt?
   c) Habt ihr die Medien nur konsumiert oder auch Inhalte produziert?
   d) Ergaben sich aus der Mediennutzung Gespräche oder Diskussionen? Wenn ja, worüber?

9. Die Medien diskutieren über die Netzneutralität. Recherchiert, was man darunter versteht und warum sie in Gefahr ist.

10. Sucht zu zweit mithilfe einer Preissuchmaschine das günstigste Angebot eines Artikels eurer Wahl. Überlegt, ob das günstigste Angebot auch das beste ist. Schreibt auf, welche Überlegungen neben dem Preis zum Kaufentschluss führen könnten. Überprüft, welche Aspekte für eure Kaufentscheidung die gewählte Preissuchmaschine nicht einblendet. Tragt die Ergebnisse eurer Recherche der Klasse vor und diskutiert, ob eure Vorgangsweise verbesserungswürdig ist.

11. Recherchiere, was am Wochenende im Kino läuft. Schreibe auf, welche Suchbegriffe du in die Suchmaske eingegeben hast. Falls die Ergebnisse unbefriedigend sind, halte auch fest, wie du die Suchanfrage verfeinern kannst.

12. Recherchiere in Wikipedia zum Südtiroler Dichter Norbert C. Kaser. Finde über die Versionsgeschichte heraus, welche Informationen mit welcher Begründung geändert wurden. Ermittle auch, ob die Verfasser des Kaser-Artikels bereits an anderer Stelle publiziert haben und ob sie von anderen Autoren zitiert werden.

13. Wie kann man bei Wikipedia die Verlässlichkeit der Informationen überprüfen?

14. Welche Vor- und Nachteile weist Wikipedia in Bezug auf Verlässlichkeit der Informationen auf?

15. Welche Medien der Provinz Bozen bieten auf ihren Webseiten kostenlose Informationen an? Recherchiere, welche Medien tagesaktuelle Informationen bereitstellen und welche im Netz auch Hintergrundinformationen liefern.

16. Recherchiert zu zweit, welche Informationen ihr bei der Verbraucherzentrale zum Thema „Kontoführung bei Südtiroler Banken“ findet. Geht zu einer lokalen Bank und informiert euch über die Spesen für ein Studentenkonto. Vergleicht im Internet, was ein Studentenkonto bei einer Online-Bank kosten würde. Stellt die Rechercheergebnisse der Klasse vor.

17. Sucht zu zweit im Netz nach einem günstigen Smartphone. Legt fest, welche Produkteigenschaften das Smartphone aufweisen sollte und findet den besten Online-Anbieter. Vergleicht eure Wahl auch mit Testergebnissen von Verbraucherzentralen. Überlegt, wie ihr mit der Phrasensuche und mit kombinierten Suchbegriffen schnell zu einer relevanten Trefferliste kommen könntet.

18. Erstellt zu dritt eine Checkliste zur Frage der Informationsqualität im Internet. Wie ist es im Internet möglich, qualitative Informationen von zweifelhaften zu unterscheiden? Was ist eine qualitativ hochwertige Information? Wie kann man zweifelhafte Informationen erkennen? Wie kann man die Verlässlichkeit von Informationen überprüfen?

19. Sucht zu zweit in Wikipedia nach drei Artikeln eurer Wahl. Prüft, ob die Artikel einen guten Überblick über das behandelte Thema liefern, ob sie ausgewogen und mit externen Quellen belegt werden. Gibt es zwischen den drei Artikeln Unterschiede in Bezug auf Verlässlichkeit? Erstellt Kriterien zur Beurteilung der Artikel und stellt diese der Klasse zur Diskussion vor.

20. Quellenkritik gehört zur Kernkompetenz jeder Internetrecherche. In diesem Fall soll Quellenkritik in Wikipedia mithilfe von Wikibu (www.wikibu.ch) geübt werden. Die Schüler wissen bereits, wie Wikipedia funktioniert, welche Zusatzinformationen sie aus der Versionsgeschichte und Diskussionsseite eines Artikels herauslesen können. Zudem wissen die Schüler, welche Zusatzinformationen der digitale Wikipedia-Assisten Wikibu zu einem Wikipedia-Artikel liefert. Ziel der Aufgabenstellung ist es, die Verlässlichkeit von Wikipedia-Artikeln zu überprüfen.

    Erster Schritt: Legt zu zweit ein Thema fest, zu dem ihr in Wikipedia nach relevanten Informationen sucht. Wählt hierzu zwei Wikipedia-Artikel aus. Erstellt Kriterien, nach denen die gewählten Artikel einer Quellenkritik unterzogen werden sollen. Haltet auch fest, warum ihr die erstellten Kriterien für sinnvoll erachtet.

    Zweiter Schritt: Jede Gruppe beurteilt auf der Grundlage der erstellten Kriterien die Verlässlichkeit der Artikel.

    Dritter Schritt: Die Gruppen recherchieren nach den wichtigsten Zusatzinformationen in der Versionsgeschichte und Diskussionsseite zu ihren gewählten Artikeln.

    Vierter Schritt: Die Gruppen überprüfen die Verlässlichkeit des Wikipedia-Artikels mithilfe von Wikibu. Sie zeigen auch auf, worin sich die Beurteilungskriterien von Wikibu von ihren eigenen unterscheiden.

Fünfter Schritt: Die relevanten Beurteilungskriterien werden schriftlich festgehalten, in der Arbeitsmappe abgelegt und an die Infotafel der Klasse geheftet.

21. Sucht zu zweit mithilfe von Wikibu nach einem Artikel, der als wenig verlässlich eingestuft wird und ermittelt, welche Faktoren dafür ausschlaggebend gewesen sein könnten.

22. Sucht zu zweit nach einem Wikipedia-Artikel, der von den Wikipedianern als subjektiv eingestuft wurde. Findet heraus, welche Informationen im Artikel als nicht neutral gewertet werden. Macht schriftlich Vorschläge, wie der Artikel neutraler formuliert werden könnte.

23. Untersucht zu zweit die Versionsgeschichte eines Wikipedia-Artikels. Ermittelt über die IP-Adresse des Autors, aus welchem Land er stammen könnte. Ist der Autor des Artikels namentlich angeführt, dann recherchiert seinen beruflichen Hintergrund und findet heraus, ob er zum behandelten Thema bereits publiziert hat.

24. Recherchiert zu zweit, welche Vorsorgebehandlung den Zähnen wirklich hilft. Welche Rolle spielt das richtige Zähneputzen? Sind elektrische Zahnbürsten wirksamer als das Putzen von Hand? Ist der Nutzen einer jährlichen professionellen Zahnreinigung erwiesen? Was heißt Fissurenversiegelung und Fluoridierung der Zähne? Für welche Behandlungsmethoden ist ein medizinischer Nutzen erwiesen ist. Ermittelt per Fragebogen das Vorsorgeverhalten eurer Mitschüler. Stellt die Ergebnisse eurer Recherche der Klasse vor und diskutiert, wie das eigene Vorsorgeverhalten verbessert werden kann. Diskutiert auch, wem man im Netz zum Thema „Vorsorgebehandlung“ mit gutem Grund vertrauen kann und was man unter „bewährten Standards“ versteht.

25. Wie sucht man bei Google nach Inhalten, die unter einer CC-Lizenz stehen?

26. Das Urheberrecht kann auch über das Stationenlernen bearbeitet werden. Bildet hierzu drei Gruppen, die unterschiedliche Aspekte des Recherchierens nach relevanten Informationen bearbeiten. Die Schüler der jeweiligen Gruppe erhalten ein Stationenschild mit Thema, Namen der Schüler sowie einen Fragenkatalog. Den Fragenkatalog sollen die Schüler jeweils um zwei relevante Fragen erweitern. Wie die Schüler ihre Antworten präsentieren, bleibt ihnen überlassen. Sie sollen aber begründen, warum sie sich für die gewählte Präsentationstechnik entschieden haben und warum sie am besten zum Inhalt passt.

    Gruppe A beschäftigt sich mit der Schulbibliothek.

    a) Wie groß ist der Bücherbestand der Schulbibliothek?
    b) Wer bestimmt, welche Bücher angekauft werden?
    c) Nach welchen Kriterien werden für die Bibliothek Bücher angekauft?
    e) …

Gruppe B beschäftigt sich mit der Erstellung einer Biographie zum Laaser Autor Franz Tumler.

a) Welche Bücher und Aufsätze hat Tumler veröffentlicht?
b) Gibt es unveröffentlichte Texte?
c) Wie erhält man Informationen über Tumlers Leben?
e) …

Gruppe C beschäftigt sich mit dem Projekt Google-Buchsuche.

a) Wie funktioniert die Google-Buchsuche?
b) Welche Bücher sind über Google-Buchsuche auffindbar?
c) Gibt es Angaben darüber, welcher Anteil der gesamten Weltliteratur von Google bereits digitalisiert wurde?
e) …

27. Kaufst du im Buchladen vor Ort ein Buch, kannst du es lesen, verschenken, verleihen oder es ungelesen für die nächsten 30 Jahre ins Bücherregal stellen. Recherchiere, welche Rechte Käufer eines E-Books geltend machen können.

28. Wer ein E-Book liest, wird u. U. überwacht; Verlage und Autoren wollen Einblick ins Leseverhalten der Käufer bekommen. Erarbeitet Antworten zu folgenden Fragestellungen:

a) Warum wollen Verlage und Autoren wissen, ob der Käufer das E-Book sofort nach dem Kauf liest, ob er es an einem Nachmittag zu Ende liest, an welchem Wochentag er das E-Book liest, welche Stellen er markiert und kommentiert, ob er parallel dazu andere Bücher liest oder ob er es nach der ersten Lesesitzung nie mehr aufruft.
b) Wie beobachten die Verlage die Nutzung von E-Books?
c) Wie erfährt ein E-Book-Leser, welche Verlage oder E-Book-Reader sein Leseverhalten ausspionieren?
d) Wie können sich E-Book-Leser vor unerwünschter Überwachung schützen?

29. Erstellt zu zweit ein Thesenpapier zur Problematik des Ranking-Systems von Suchmaschinen.

a) Stellt in Form von Kurzthesen die gängige Kritik zum Ranking-System von Google zusammen.
b) Stellt das Projekt „Wikia Search“ als Alternative zum Google-Ranking vor. Welche Grundsätze tragen „Wikia Search“? Welche Schwächen weist „Wikia Search“ auf?

30. Stellt in Kurzform die Standards des Qualitätsjournalismus auf. Wählt eine Online-Zeitung mit Kommentarfunktion aus. Analysiert drei Leserkommentare, inwieweit diese den journalistischen Standards entsprechen.

31. Recherchiert im Fach Ökonomie zum Thema „Krisenmanagement der EU zur Staatschuldenkrise“ und ermittelt, wer hinter den Web-Angeboten steht.

    a) Welche Webseiten informieren neutral über das bisherige Krisenmanagement der EU?
    b) Welche Webseiten bewerten das bisherige Krisenmanagement als „alternativlos“?
    c) Welche Webseiten bieten alternative Konzepte zur Bekämpfung der Staatsschuldenkrise an?
    d) Welche Webseiten sehen im Euro selbst die Ursache für die Staatsschuldenkrise und fordern die Rückkehr zu nationalen Währungen?

32. Enthüllungsplattformen wie WikiLeaks[75] oder anonyme digitale Redaktionsmailboxen wie die der ZEIT Online[76] werfen das Problem des Quellenchecks im digitalen Umfeld auf.

    a) Welche Kompetenzen sollte ein Journalist aufweisen, um anonyme digitale Quellen bearbeiten und verwenden zu können?
    b) Macht euch bei Journalisten lokaler Medien kundig, wie sie mit anonymen Quellen umgehen. Wie verifizieren Journalisten anonyme Quellen? Wann ist für Journalisten eine Quelle glaubhaft?
    c) Wie können Leser überprüfen, ob die dargebotenen Informationen der Journalisten verlässlich sind? In welchen Fällen sollten Leser auch gegenüber dem Journalismus ein gesundes Misstrauen an den Tag legen? Verfasst zum Thema „Quellencheck“ Tipps für den Lesealltag.

33. Die Schulbibliothek will einen E-Book-Reader kaufen. Die Bibliothekarin ersucht um Tipps bei der Wahl des richtigen E-Book-Readers.

    a) Erstellt relevante Kaufkriterien für den E-Book-Reader und begründet eure Entscheidungen.
    b) Wo erfährt man, was man mit einem E-Book-Reader alles machen kann?
    b) Wo kann man sich informieren, welche Formate die jeweiligen E-Book-Reader verstehen?
    c) Gibt es Software, die Formate für E-Books in alle wichtigen Formate konvertieren kann?

34. Bei der Internetrecherche stellt sich das Problem, wie man Unwichtiges von Relevantem oder Verlässliches von Gerüchten trennt. Wie filtert die Suchmaschine Google aus der Flut der Informationen die relevante Information?

35. Experten behaupten, dass etwa ein Drittel der Hotelbewertungen gefälscht ist. Erstellt eine Checkliste, die dem Verbraucher bzw. euch bei der nächsten mehrtägigen Klassenfahrt hilft, echte von gefälschten Bewertungen und Kommentaren zu unterscheiden.

75 http://www.wikileaks.org
76 http://www.zeit.de/briefkasten/index.html

a) Verfasst eine Checkliste zur Bewertung der Qualität des Bewertungssystems. Sucht nach einem Bewertungssystem, das euren Maßstäben nicht entspricht und eines, das das sie erfüllt.
b) Verfasst eine Checkliste zur Einschätzung der Bewertungen und Kommentare der Hotelgäste. Welche Bewertungsmerkmale deuten auf bezahlte Marketingagenturen hin? Sucht nach typischen gefälschten Bewertungen.

36. „Sharing Economy“, die Ökonomie des „Teilens und Tauschens“, verändert offenbar die Wirtschaftswelt. Eine Gruppe von Schülern befasst sich mit folgenden Rechercheaufgaben:

a) Welche Formen der Sharing Economy gibt es?
b) Welche Risiken sind mit der Sharing Economy verbunden?
c) Recherchiert nach Blogs, die sich mit dem Thema „Sharing Economy“ befassen.
d) Recherchiert, ob es in der Region Sharing-Projekte gibt und wie sie funktionieren.
e) Zeigt, wie man mithilfe der Firefox-Erweiterung Sage zum Thema „Sharing-Economy“ auf dem Laufenden bleibt.
f) Zeigt, wie man mit dem RSS-Reader The Old Reader auf dem Laufenden bleibt und wie man beispielsweise mit der Android-App gReader auch mobilen Zugriff auf The Old Reader hat.

37. Der Buchautor Eli Pariser vertritt die These, dass das personalisierte Internet eine „Filter Bubble“ erzeugt. Nutzer bekommen im Netz nur noch das zu sehen, was zu ihrem Netz-Profil passt. Die II-Konzerne verfolgen dabei unterschiedliche Filter-Ansätze, um das „wahre Ich“ des Nutzers zu ermitteln.

a) Auf welche Filtersysteme setzen Google, Facebook oder Amazon?
b) Wo liegen die Schwächen und Stärken der einzelnen Filter-Ansätze bei der Frage, wer der einzelne Nutzer wirklich ist?
c) Wie sollte die Politik auf das Personalisieren reagieren: Laissez-faire, Verbot, Pflicht zur Offenlegung der Filtersysteme, Möglichkeit für den Nutzer die Personalisierung abschalten zu können?
d) Wie kann sich der Nutzer selbst vor unerwünschten Personalisierungen schützen?

2 Digitales Publizieren und Recht

Leitfragen

- Was unterscheidet das Web 1.0 vom Web 2.0?
- Welche Rechte stehen den Kreativen im Netz zu?
- Gibt es Alternativen zum klassischen Urheberrecht?
- In welchen Fällen können Nutzer ohne Erlaubnis der Rechteinhaber deren Werke nutzen?
- Welches sind die wichtigsten Regeln für die Quellenangaben von geschützten Medieninhalten?
- Welche Rechtsnormen musst du bei der Erstellung von Texten, Fotos, Videos oder Audios beachten?
- Wie kannst du beim Publizieren unerwünschte Datenspuren verhindern?
- Wie kannst du im Netz das Recht auf „informationelle Selbstbestimmung“ durchsetzen?

Das Internet ermöglicht uns heute nicht nur nach Informationen zu suchen, sondern auch als Anbieter von Informationen aufzutreten. Der Nutzer konsumiert nicht mehr nur Inhalte, die andere bereitstellen, sondern stellt als Prosument selbst Inhalte bereit. Der Wandel vom Konsumenten zum Produzenten wird gerne als Wandel vom Web 1.0 zum Web 2.0 beschrieben. Unter dem Schlagwort Web 2.0 werden Techniken des „Mitmachens“ verstanden, wie Fotos auf Flickr hochladen, einen Artikel in Wikipedia bearbeiten, ein Weblog betreiben, einen Podcast erstellen, an einem Forum teilnehmen oder auf sozialen Netzwerken Infos tauschen. Einfachste und weitgehend kostenlose Software ermöglicht, dass eine neue digitale Öffentlichkeit „von unten“ entstehen kann.

Willst du deine Werke ins Netz stellen, solltest du die rechtlichen Rahmenbedingungen für das digitale Publizieren kennen, um keinen Ärger durch kostspielige Abmahnungen zu riskieren. Es ist nämlich nicht so ohne weiteres erlaubt, per Handy ein Videoclip zu erstellen, Fotos nach Belieben zu knipsen und beides auf soziale Plattformen hochzuladen. Ebenso ins Auge gehen kann, wenn du CDs rippst und die Audiofiles ins passende Format für deinen MP3-Player bringst und sie per Filesharing mit Freunden tauschst. Dieses Kapitel liefert dir einen groben Überblick über das Urheberrecht (Legge 633/1941), das gewissermaßen den ersten Teil der „Magna Charta“ der Informationsgesellschaft bildet. Der Überblick soll dir helfen, die juristischen Stolpersteine zu umgehen, die bei der Medienproduktion auftauchen können. Du erfährst auch,

dass es zum klassischen Urheberrecht juristische Alternativen gibt, wie die Creative Commons-Lizenz, die besser zur Kultur der Kooperation und des Remix passen.

Wer fürs Web 2.0 produziert, berührt auch unweigerlich datenschutzrechtliche Fragen. Im Netz kann die digitale Privatsphäre schnell verletzt werden, indem Nutzer ohne Einverständnis der Betroffenen E-Mail-Adressen auf Facebook hochladen oder Metadaten preisgeben, die für die Publikation der eigenen Werke nicht erforderlich wären. Du kannst dich darüber informieren, wie du bei der Mitgestaltung der digitalen Welt die Privatsphäre anderer Personen achten und die Kontrolle über deine persönlichen Daten behalten kannst. Der wirksame Datenschutz (D.lgs. 196/2003) zählt zum zweiten Teil der „Magna Charta" der Informationsgesellschaft.

2.1 Das Urheberrecht

2.1.1 Schutz des Urhebers

2.1.1.1 Wer ist Urheber?

> *„Geistiges Eigentum ist die Rechtsform des Informationszeitalters"*
> James Boyle, Rechtswissenschaftler

Urheber ist, wer ein Werk schafft. Werke können Texte, Reden, Fotos, Filme, Musik oder auch Computerprogramme sein; sie sind urheberrechtlich geschützt, sofern sie ein gewisses Maß an Originalität aufweisen. Wer fremde Werke übernimmt, also Texte anderer Autoren abschreibt oder den Quellcode fremder Software in die eigene importiert, ist kein Urheber. Das Urheberrecht entsteht mit dem tatsächlichen Schaffensvorgang; erforderlich ist weder eine Eintragung in öffentliche Register noch ein Urheberrechtsvermerk (©, Jahr, Urheber oder Rechteinhaber). Unerheblich ist auch, wo das Werk veröffentlicht wird. Texte, die in eine Online-Zeitung hochgeladen werden, sind gleichermaßen geschützt, wie solche, die etwa in einer Tageszeitung abgedruckt werden. Haben mehrere Personen gemeinsam ein Werk geschaffen, so werden sie zu Miturhebern. Das ist etwa bei Multimediawerken der Fall, wenn mehrere Personen an der Herstellung des Werkes beteiligt sind, wie Texter, Fotografen, Filmer und Musiker.

Ideen genießen keinen Urheberschutz. Wer nur die Idee hat eine App zu programmieren, die zum momentanen Standort Restaurants mit regionaler Küche anzeigt, sie aber nicht umsetzt, hat keinen Anspruch auf Urheberschutz. Die Ideen sind gemeinfrei und können von allen nach Belieben genutzt werden. Frei sind auch die Ideen, die einem schutzfähigen Werk zugrunde liegen. Jeder kann die Idee einer Restaurant-App auf-

greifen und selbst eine App erstellen, mit einer eigenen klareren Programmoberfläche, neuen Funktionen und mehr Schutz der digitalen Privatsphäre.

Der Urheberschutz ist kein ewiges Recht, er ist zeitlich begrenzt. 70 Jahre nach dem Tod des Urhebers erlischt es und wird gemeinfrei. Starb ein Schriftsteller am 23. Juni 1942, so begann die Schutzdauer am 1. Jänner 1943 und endete am 31. Dezember 2012. Jährlich vergrößert sich so der Pool an gemeinfreien Werken von Autoren, Komponisten oder Wissenschaftlern.[77]

2.1.1.2 Welche Rechte hat der Urheber?

Urheberpersönlichkeitsrechte

Das Urheberrecht umfasst sowohl Urheberpersönlichkeitsrechte als auch Verwertungsrechte. Das Urheberpersönlichkeitsrecht schützt die ideellen Interessen des Urhebers. Der Urheber hat das Recht zu entscheiden, ob, wann oder wo er sein Werk erstmals veröffentlichen will. Der Autor eines Textes kann selbst darüber bestimmen, ob er sein Werk im Internet zum Download für E-Books anbietet, es einem Verlag sendet für eine eventuelle Printausgabe oder bei einem literarischen Abend Auszüge daraus vorliest.

Der Urheber hat weiter ein Recht auf Namensnennung; er kann also frei bestimmen, ob das Werk ohne Namen, unter seinem Namen oder unter einem Pseudonym veröffentlich wird. Schließlich beinhaltet das Urheberrecht das Recht auf Integrität des Werkes, und zwar gegen unerlaubte Bearbeitungen oder Ergänzungen. Der Urheber hat das Recht gegen den Bearbeiter seines Fotos vorzugehen, der mithilfe eines Bildbearbeitungsprogramms dieses ohne seine Zustimmung verändert hat (vgl. Foto 1 und 2). Das unbearbeitete Foto darf auch nicht in einen gänzlich unerwünschten Kontext gestellt werden; so darf zum Beispiel das Porträt einer Pazifistin nicht für die Interessen der Waffenlobby vereinnahmt werden.

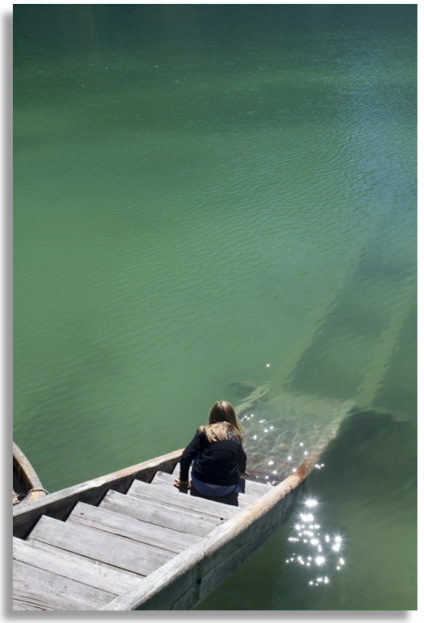


Foto 1: unbearbeitetes Foto

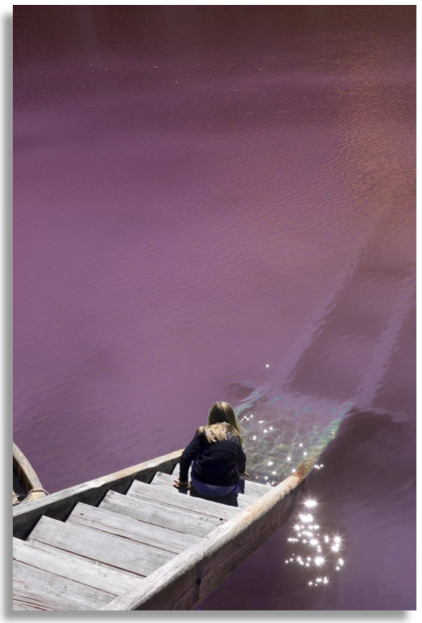


Foto 2: unerlaubte Fotobearbeitung

77 http://www.heise.de/tp/artikel/38/38241/1.html

Verwertungsrechte

Die Verwertungsrechte schützen die wirtschaftlichen Interessen des Urhebers. Grundlage für den Verwertungsanspruch bildet die Eigentumsgarantie in der Verfassung (Art. 42); man spricht auch vom „geistigen Eigentum“ des Urheberrechts. Wer Urheber ist, kann darüber bestimmen, ob das Werk vervielfältigt und verkauft wird und wer das Werk wann, wo und wie nutzen darf. Die Übertragung der Nutzungsrechte an andere erfolgt über einen Lizenzvertrag. Eine wichtige Unterscheidung hierbei ist die zwischen einfachen und ausschließlichen Nutzungsrechten. Einfache Nutzungsrechte kannst du so oft vergeben, wie du willst. Du kannst dasselbe Foto einer Online-Zeitung und einem Fotoverlag verkaufen. Das ausschließliche Nutzungsrecht kannst du nur einmal vergeben. Nur der Inhaber der Lizenz ist dann berechtigt, das Foto zu nutzen; du als Fotograf darfst dann das lizenzierte Foto nicht einmal auf deinem Weblog veröffentlichen. Lizenzen legen den Umfang und die Art der erlaubten Nutzung fest. So können etwa Softwarelizenzen, wie die EULA von Microsoft, vorsehen, dass das Programm nur für private Zwecke und nur auf einem einzelnen PC genutzt werden darf. Ist der Kreative als Programmierer angestellt, stehen die Nutzungsrechte an der Software nicht dem Programmierer zu, sondern alleine dem Arbeitgeber. In diesem Fall entscheidet der Arbeitgeber, wie die Software genutzt und vermarktet werden darf.

Eula Office 2013

Die Einzellizenz für MS Office 2013 war ursprünglich an einen PC gebunden. Die Nutzer waren nicht berechtigt, „die Software auf einen anderen Computer oder Nutzer zu übertragen.“ Anfang März 2013 änderte Microsoft die Lizenzbestimmungen aufgrund von „Kundenrückmeldungen“ und erlaubte wieder, dass Office 2013 - nach vorheriger Deinstallation - auch auf einem anderen PC installiert werden kann.

2.1.1.3 Was ist das Hausrecht?

Das Hausrecht steht dem Inhaber von Räumlichkeiten zu. Der Inhaber kann ausschließlich festlegen, wer seine Wohnung betreten darf, wie sie genutzt werden darf, ob in der Wohnung fotografiert oder gefilmt werden darf. Wenn der Inhaber will, kann er auch ohne Angabe von Gründen ein Hausverbot aussprechen. Willst du etwa in einem Museum, einem Kino, einem Schloss oder in einer privaten Wohnung ein Foto machen, musst du den Inhaber dazu um Erlaubnis fragen.

Zulässig hingegen ist, Außenaufnahmen eines Bauwerkes von öffentlichen Straßen und Plätzen zu machen und die Fotos dann ins Netz zu stellen. Die Fotos dürfen nur in Augenhöhe gemacht werden, also ohne Hilfsmittel wie Leiter oder Heißluftballon. Auch dürfen nicht von einem gegenüberliegenden Haus aus Fotos von der Grillanlage im Garten privater Ferienhäuser gemacht werden.

2.1.2 Schutz des Nutzers

2.1.2.1 Interessen im Urheberrecht

Das Urheberrecht regelt Herstellung, Vermarktung und Nutzung der schöpferischen Güter. Das Verhältnis zwischen den Akteuren des schöpferischen Marktes ist konfliktgeladen. Die Urheber haben ein Interesse am ungehinderten und möglichst kostenlosen Zugriff auf Kulturgüter, um diese als Anregung für ihre eigene kreative Arbeit nutzen zu können. Die Vermarkter, also Musikkonzerne, Softwarehäuser oder Verlage haben ein Interesse daran, mit kreativen Gütern profitable Geschäfte zu machen. Die Allgemeinheit schließlich hat ein Interesse an einer Vielfalt an schöpferischen Gütern und auch daran, diese kostengünstig zu nutzen. Der ungehinderte Zugriff auf Kulturgüter ist elementar, weil sie die Grundlage für Bildung, öffentliche Diskurse und informierte Entscheidungen in Alltag, Beruf und Politik bilden. Die italienische Verfassung sieht deshalb auch vor, dass sich die Privatinitiative nicht im Gegensatz zum „Nutzen der Allgemeinheit“ betätigen darf (Art. 41 II Verf.).

Im Interesse der Allgemeinheit setzt das Urheberrecht dem „geistigen Eigentum“ Grenzen. Kreative und Nutzer dürfen fremde Leistungen in bestimmten Fällen ungefragt nutzen. Das Urheberrecht spricht von gesetzlichen Lizenzen.

2.1.2.2 Privatkopie

Die Suchergebnisse kannst du grundsätzlich als Privatkopie sichern, sofern sie nicht kopiergeschützt sind. Den Medienanbietern dienen die Kopierschutzmaßnahmen dazu, ihre Absatzinteressen zu schützen, also zu bewirken, dass nur derjenige, der zahlt, Zugriff auf die digitalen Güter hat. Erlaubt sind auch Mitschnitte der Musiktitel von einem Internet-Radio. Dasselbe gilt für Podcasts; sie werden zum automatischen Download angeboten, dass sie auf einem portablen MP3-Player zu jedem beliebigen Zeitpunkt angehört werden können. Ebenso zulässig ist der direkte Tausch von geschützten Inhalten wie Texten und Fotos per Handy über Bluetooth, soweit dieser nur privaten Zwecken dient. Der private Tausch stellt nämlich urheberrechtlich keine zustimmungspflichtige Veröffentlichung dar.

Software	Webadresse	Besonderheiten
gPodder	http://gpodder.org	gPodder ist ein Podcastmanager, mit dem man manuell oder nach einem Zeitplan Audiodateien auf den PC herunterladen kann.
MusicBee	http://www.getmusicbee.com	MusicBee ist ein Musikplayer, der den Zugriff auf Webradios, Podcasts sowie CD-Ripping ermöglicht.
streamWriter	http://streamwriter.org/de	streamWriter ist ein Programm, mit dem man Audiostreams der Internet-Radios aufzeichnen und als MP3-Dateien auf der Festplatte abspeichern kann.

Tab. 05: Radiomitschnitte und Podcatcher

In Italien darfst du von geschützten MP3-Dateien nur dann eine Privatkopie erstellen, wenn du selbst im Besitz der Original-MP3-Datei oder der Original-CD bist. Dies bedeutet, dass du dir kein digitales Musikarchiv von geschützten MP3-Dateien über Tauschbörsen (Peer-to-Peer-Netzwerken) oder per Download von Filehostern anlegen darfst, weil dies dich in Konflikt mit dem Urheberrecht bringt und du möglicherweise eine kostenpflichtige Abmahnung vom Anwalt riskierst.

Für Software, die auch unter das klassische Urheberrecht fällt, ist kein Recht auf Privatkopie vorgesehen. Du darfst lediglich von der gekauften Software „eine einzige“ Sicherheitskopie erstellen, falls etwa der Verkäufer des Notebooks keine Recovery-CD mitgeliefert hat. Crasht das Betriebssystem, kannst du es mithilfe der Recovery-CD wiederherstellen. Anders verhält es sich bei Open-Source-Software; sie darfst du nach Belieben kopieren, verbreiten und in der Regel auch weiterentwickeln.

Darf man auf Videoportalen wie YouTube[78] Videos anschauen, die urheberrechtlich bedenklich sind? Beim sogenannten Streaming werden lediglich temporäre Kopien im Arbeitsspeicher und im Cache abgelegt. Rechtlich unklar ist bis heute, ob bereits ein flüchtiges Speichern eine unerlaubte Vervielfältigung darstellt und somit illegal wäre oder erst das dauerhafte Speichern auf dem eigenen Datenträger. Andererseits enthält das Urheberrecht kein Verbot, ein fremdes Werk zu lesen, anzuhören oder anzusehen. Sollte ein flüchtiges Speichern von illegalen Videos im Cache rechtswidrig sein, dann dürfte die Rechtsverfolgung des Streaming-Nutzers durch den Rechteinhaber des Videos schwierig sein, weil der Nutzer nur anhand der IP-Adresse identifiziert werden kann. Im Besitz der IP-Adresse und den Bestandsdaten der Nutzer sind die Provider, die diese nur per Gerichtsbeschluss herausgeben müssen. Zudem muss der Rechteinhaber zweifelsfrei die Filmkopie im temporären Speicher des PCs oder Smartphones nachweisen.

78 https://www.youtube.com/

2.1.2.3 Zitate und Links

Eine weitere Schranke des Urheberrechts ist das Recht, aus anderen Werken zitieren zu dürfen. Zulässig ist ein Zitat, wenn es nur Beiwerk eines eigenständigen Werkes ist; die Eigenleistung des eigenen Werkes muss im Vordergrund stehen. Das Zitat muss der geistigen Auseinandersetzung mit dem zitierten Werk dienen und der Umfang ist auf das unbedingt erforderliche Maß zu begrenzen. Nicht erlaubt ist etwa, 100 fremde Fotos für ein Fotobuch zu verwenden, weil hierbei eine geistige Beschäftigung mit den fremden Fotos fehlt. Erlaubt hingegen ist, eine Rezension zu einem Fotobuch im eigenen Weblog zu schreiben und als Beleg ein oder zwei Fotos aus dem Fotobuch ins Netz zu stellen. Zulässig ist auch, einen Artikel zum Krisenmanagement der EU zur Finanzmarktkrise zu schreiben und die eigene Meinung mit einem Zitat des Experten XY zu stützen und mit Daten vom Statistischen Amt der Europäischen Union (Eurostat) zu belegen. Übernehmen Autoren fremde Textstellen wörtlich, müssen sie diese kennzeichnen, damit der Leser nachvollziehen kann, was von wem im Einzelnen stammt. Geben Autoren Gedanken anderer mit eigenen Worten wieder, müssen sie auch das kennzeichnen.

Wie ist die Verlinkung von Webseiten urheberrechtlich zu bewerten? Links sind nicht zustimmungspflichtig, sofern die verlinkten Webseiten frei zugänglich sind.[79] Im Grunde stellt die Verlinkung selbst bereits eine Quellenangabe dar. Verstoßen Nutzer gegen das Urheberrecht, wenn sie YouTube-Videos in ihre eigene Webseite einbetten? Bei Frames können nämlich die Nutzer nicht auf den ersten Blick erkennen, dass es sich um fremde Werke handelt. Der Europäische Gerichtshof (EuGH)[80] hat entschieden, dass „framende Links“ nicht Urheberrecht verletzen. Voraussetzung dafür ist aber, dass das Video auf YouTube „für alle Internetnutzer frei zugänglich ist“ und dass der Nutzer, der das Online-Video in seinen Blog einbettet, dazu nur den offiziellen YouTube-Player verwendet.

79 EuGH C-466/12 Urteil vom 13.2.2014: http://curia.europa.eu/juris/document/document.jsf?text=&docid=147847&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=77208

80 EuGH C-348/13 Beschluss vom 21.10.2014: http://curia.europa.eu/juris/liste.jsf?num=C-348%2F13

Richtige Quellenangabe

Hier die wichtigsten Regeln für richtige Quellenangabe im Überblick. Die kursiven Begriffe sind als Platzhalter zu verstehen.

Bücher:

- **Vollbeleg:** *Autor(en) (Jahr): Titel. Untertitel, Ort X. Auflage (Jahr der Erstauflage), Seite*. Z. B. Hosseini, Khaled (2003): *Drachenläufer,* Berlin, S. 201. *Nachname, Vorname:* Bei mehreren Autoren wird nur der erste genannt und mit „u. a." auf die restlichen verwiesen. Erscheinungsjahr: *(Jahr).* Titelangabe: *Titel. Untertitel.* Erscheinungsort *(Ort)*: Bei mehreren Erscheinungsorten ist nur der erste Ort anzugeben und „u. a." hinzuzufügen. *Auflagennummer, Jahr der Neuauflage (Jahr der Erstauflage):* Bei einer Neuauflage wird dem Jahr der Neuauflage die hochgestellte Auflagennummer vorangestellt und das Jahr der Erstauflage in runden Klammern angeführt, z. B. ^{2}2013 (2003). Der Vollbeleg scheint in der Regel im Literaturverzeichnis auf.
- **Kurzbeleg:** *Nachname des Autors (Jahr): Kurztitel, Seite.* Erlaubt ist auch: *Nachname des Autors: „a.a.O."* (= am angegebenen Ort), *Seite*. Anwendung finden auch extreme Kurzformen des Anmerkungsapparates: *Nachname (Jahr: Seite)*. Z. B. Hosseini (2003: 126). Kurzbelege finden sich in der Regel im Fließtext oder in der Fußzeile.

Fachzeitschriftenaufsatz:

Autor (Jahr): Titel, in: Zeitschrift Erscheinungsjahr, Heftnummer, Seite. Z. B. Würth, Anna u. a. (2012): *UN-Kinderrechtskonvention: Der normative Rahmen,* in APuZ 43/2012, S. 28-34.

Presse:

Autor bzw. ohne Verfasser (o. V.) *(Jahr): Titel, in: Zeitung, Nummer, Datum, Seite.* Z. B. Müller, Martin U. u. a. (2012): *Der Türsteher,* in: Der Spiegel 43/2012, S. 86-94.

Rundfunksendungen:

Titel der Sendung. Gestaltung: Vorname Name. Sender, Sendedatum, Uhrzeit. Z. B. Computer & Kommunikation. Manfred Kloiber. Deutschlandfunk, 20.07.2013, 16:30-17:00 Uhr.

Fernsehsendungen:

Titel der Sendung (Jahr), Sender, Regie (Vorname, Name), Sendedatum, Uhrzeit. Z. B. Ziemlich beste Freunde (2014), DAS ERSTE, Regie Olivier Nakache u. a., 07.07.2014, 20:15 Uhr, 112 Min.

Regeln für korrektes Zitieren

1. **Zitate im Text:** Sie müssen durch doppelte Anführungszeichen zu Beginn und am Ende des Zitats kenntlich gemacht werden. „Der Gemeingüterbegriff hilft, unsere Nutzungsoptionen gemeinsamer Ressourcen zu erweitern …"
2. **Platzierung der Fußnote:** Bezieht sich die Fußnote auf einen vollständigen Satz, steht sie nach dem abschließenden Satzzeichen. Bezieht sich die Fußnote nur auf ein Wort oder einen Satzteil, steht sie hochgestellt unmittelbar hinter dem betreffenden Wort oder Satzteil.
3. **Zitat im Zitat:** Enthält der zitierte Satz selbst ein Zitat, wird dieses beim Zitieren durch einfache Anführungszeichen (‚…') gekennzeichnet.
4. **Auslassungen im Zitat:** Sie sind im Zitat durch […] zu kennzeichnen und nur erlaubt, wenn sie den Sinn des Satzes nicht verfälschen.
5. **Zitierte Titel:** Im laufenden Text ist der zitierte Titel im Original beizubehalten; z. B. die Stiftung Warentest fasst in ihrer Zeitschrift test 6/2012 den Datenschutz bei Apps mit dem Satz zusammen …

Videos:

Titel (Erscheinungsjahr). Autor oder Regisseur. Form (Blu-ray, DVD, VHS Video), Spieldauer, Vertrieb. Z. B. *Die sieben Schwerter* (2010). Tsui Hark. Blu-ray, 155:10 Min., Universum Film.

Fotos:

Name (des Fotografen)*: Titel* (ist kein Titel vorhanden: *o. T.* = ohne Titel), *Entstehungsjahr* (ist kein Jahr angegeben: *o. J.* = ohne Jahresangabe). Weitere Angaben hängen vom Medium ab, in dem das Foto veröffentlicht wurde; also ob es etwa aus einem Buch, einer Zeitung oder dem Internet stammt. Quellenangaben bei Fotos von Fotoagenturen: *Foto: Agentur – Name* (des Fotografen): *Titel, Entstehungsjahr.* Bei Fotos, die unter einer CC-Lizenz stehen und im Netz veröffentlicht werden, sind der Textlink zum Foto, zum Namen des Fotografen und zur Lizenz anzugeben: *z. B. Foto: Jörg Hempel, Lizenz: CC BY-SA 3.0 de.*

Web-Dokumente:

- **Webseite:** Bei einem HTML-Dokument gilt: *Autor (Jahr): Titel, Webadresse, Erscheinungsdatum, Uhrzeit, (Abrufdatum). Z.* B. Schmidt-Häuer, Christian (2011): *Amerikas Schande,* http://www.zeit.de/2011/03/USA-Guantanamo, 16.01.2011, 18:34 Uhr (24.07.2012). Das Abrufdatum ist erforderlich, weil Web-Dokumente verändert und aktualisiert werden können.
- **PDF-Dokument:** Bei einem PDF-Dokument kommt noch die Seitenzahl hinzu: *Autor (Jahr): Titel, Webadresse, Erscheinungsdatum, Uhrzeit, Seite.* Z. B. Sieling, Carsten (2012): *Finanztransaktionssteuer. Sinnvoll, machbar, überfällig,* http://www.fes.de/ipa/inhalt/publikationen.php, März 2012, S. 2.
- **Dynamische Webseite:** Bei Webseiten, die ihre Inhalte variieren, wie Weblogs oder Wikis: *Webadresse (Abrufdatum).* Als Beleg kann die betreffende Webseite entweder lokal als PDF-Datei oder bei einem Dienst wie „WebCite“[81] archiviert werden. In diesem Fall wird im Zitat die Webadresse der archivierten Webseite angegeben.
- **Wikipedia:** Bei Wikipedia sollte neben der CC-Lizenz auch die Artikel-Version angeführt werden, damit der Leser nachvollziehen kann, auf welchen Inhalt sich der Quellenbeleg bezieht. Am einfachsten ist, der Zitierempfehlung von Wikipedia zu folgen. Rufe dazu die Wikipedia-Seite des Artikels auf. Links unter der Menübox *Werkezeuge* findest du den Navigationspunkt *Seite zitieren*. Klicke darauf und du erhältst unter „Einfache Zitatangabe zum Kopieren“ eine Kopiervorlage für die Quellenangabe zum geöffneten Artikel. Eine Quellenangabe zum Südtiroler Dichter Norbert C. Kaser würde so aussehen: „Norbert Conrad Kaser“. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 4. Mai 2015, 09:26 UTC. URL: http://de.wikipedia.org/w/index.php?title=Norbert_Conrad_Kaser&oldid=141755519 (Abgerufen: 11. Juni 2015, 16:32 UTC)

Podcasts:

Autor (Jahr): Titel. Untertitel, Webadresse, Erscheinungsdatum, Uhrzeit. Z. B. Marcus Richter (Moderation), Dodger, Constanze Kurz (2012): *Einmal mit Profis. Wenn Hacker Politik machen,* CR180, http://chaosradio.ccc.de/cr180.html, 29.06.2012, 12:50 Uhr.

81 http://www.webcitation.org/

Interviews:

Name, Vorname (Jahr): Interview, danach folgt eine Kurzbeschreibung der Berufsbezeichnung und der Position im Unternehmen oder in der Behörde des Interviewpartners, *Datum und Uhrzeit des Interviews, Webadresse.* Z. B. Snowden, Edward (2013): Interview, ehemaliger IT-Techniker für Auftragnehmer des US-Geheimdienstes NSA, 10.06.2013, 14:32 Uhr, http://www.freitag.de/autoren/the-guardian/wir-ueberwachen-jeden-ueberall

E-Mails:

Verfasser, Betreff der E-Mail, <E-Mail-Adresse>; ist der Absender nicht der Verfasser: *Verfasser, Betreff der E-Mail, E-Mail von Name des Absenders <E-Mail-Adresse> (Absendedatum).*

2.1.2.4 Schulgebrauch

Im Interesse der Bildungschancen erlaubt das Urheberrecht, geschützte Texte für den Schulunterricht zu kopieren. Teile fremder Textwerke sowie einzelne Artikel aus Zeitungen oder Blogs dürfen zu Unterrichtszwecken ohne Erlaubnis des Autors oder Rechteinhabers digital gesichert und in Klassenstärke vervielfältigt werden. Die Lehrkräfte sind allerdings verpflichtet, Autor, Titel und Internetadresse des kopierten Werkes anzuführen. Sind die Texte kopiergeschützt, dürfen sie nicht im Unterricht genutzt werden. Eine Umgehung des Kopierschutzes ist auch für die Schule nicht erlaubt.

Wikipedia-Artikel sind für den Schulgebrauch gänzlich unproblematisch, sie stehen unter der CC-Lizenz und können deshalb ohne Einschränkung gelesen, kopiert, veröffentlicht und auch bearbeitet werden.

2.1.2.5 Öffentliches Informationsinteresse

Erst eine umfassende Information ermöglicht die freie Meinungsbildung der Bürger und die fundierte öffentliche Debatte über politische Fragen. Der Gesetzgeber berücksichtigt dies im Urhebergesetz und sieht für öffentliche Reden und Zeitungsartikel Nutzungsprivilegien vor.

Die Presse darf öffentliche Reden, wie z. B. jene, die bei einer 1.-Mai-Kundgebung gehalten werden, verbreiten, muss aber den Redner, das Datum und den Ort der Rede angeben. Das Urheberrecht nennt ausdrücklich Tageszeitungen und Zeitschriften als Träger der gesetzlichen Lizenz. Die Entwicklung des Web 2.0 würde es jedoch nahelegen, dass es auch den Neuen Medien wie Weblogs erlaubt sein müsse, die digitale Öffentlichkeit über solche Reden zu unterrichten. Nicht zu öffentlichen Reden zählen Ansprachen, die auf internen Versammlungen gehalten werden, wie etwa auf Betriebsversammlungen oder Hauptversammlungen einer

AG. Der Veranstalter einer internen Versammlung könnte auch auf der Grundlage seines Hausrechts den Mitschnitt von Ansprachen untersagen.

Weiters dürfen einzelne Presseartikel, die sich schwerpunktmäßig mit wirtschaftlichen, politischen und religiösen Tagesfragen beschäftigen, von anderen Tageszeiten oder Zeitschriften übernommen werden. Artikel zu kulturellen und wissenschaftlichen Fragen fallen nicht unter die gesetzliche Lizenz. Versieht ein Autor seinen Artikel mit einem Vorbehalt der Rechte, dann darf der Artikel nicht ohne dessen Zustimmung veröffentlicht werden.

Erlaubt ist auch der elektronische Pressespiegel. Hierbei handelt es sich um Presseauszüge, die den Tagesinteressen aus Wirtschaft, Politik und Religion Rechnung tragen. Nicht unter die Lizenz des Pressespiegels fallen Fotos, Zeichnungen oder Kurzfilme.

Offen ist derzeit der Rechtskonflikt zwischen dem News-Dienst von Google[82] und zahlreichen Online-Tageszeitungen. Darf Google ohne Erlaubnis der Rechteinhaber Überschriften, Artikel-Anrisse und Links zu den Texten in den Onlineausgaben der Zeitungen setzen, zu Themenblöcken sortieren und über seinen News-Dienst verbreiten? Die Presseunternehmen sehen hierbei einen Verstoß gegen das Urheberrecht, weil Google fremde Inhalte für eigene Geschäftsmodelle nutzt. Google argumentiert dagegen, dass in Google News nur die Überschriften und die ersten Zeilen des Artikels erscheinen. Wer den gesamten Artikel lesen möchte, muss die Webseite der Zeitung aufrufen.

2.1.3 Creative Commons[83] – Lizenz fürs Internet

> *„Jeder erhält die Erlaubnis, das Programm zu benutzen, es zu kopieren, zu modifizieren und modifizierte Versionen zu vertreiben. Aber keine Erlaubnis, der Lizenz eigene Restriktionen zuzufügen. Auf diese Weise müssen die Produzenten proprietärer Software draußen bleiben."*
>
> Richard Stallman, Begründer der Freie-Software-Bewegung

Ein wachsender Teil der Softwareentwickler, Musiker, Fotografen, Autoren und Wissenschaftler stellt seine kreativen Inhalte unter freie Lizenzen. Die Motive dafür sind unterschiedlich. Manche wollen damit zeigen, dass sie sich für einen freien Zugang zu Kulturgütern und Informationen aussprechen. Andere haben ein Interesse daran, dass ihre Werke bearbeitet, weiterentwickelt und frei genutzt werden können. Auch Geschäftsinteressen können das treibende Motiv bilden. Junge Künstler und Autoren bieten ihre kreativen Inhalte aus Aufmerksamkeitsgründen gratis an, um dadurch schneller bekannt zu werden.

82 https://www.google.com/news
83 https://creativecommons.org. Was ist CC? http://de.creativecommons.org/was-ist-cc/

Pioniere freier Lizenzen, also frei von den Fesseln des „geistigen Eigentumsrechts“, waren Programmierer in den 1980er Jahren. Das bekannteste Beispiel für freie Software-Lizenzen ist die GNU General Public License (GPL), die 1989 vom Programmierer Richard Stallman entwickelt wurde.[84]

Im Jahre 2001 gründete der Rechtsprofessor Lawrence Lessig die gemeinnützige Lizenzierungsplattform Creative Commons. Die Plattform bietet auf ihrer Webseite die Creative-Commons-Lizenz („CC-Lizenz“) an, mit deren Hilfe Autoren, Musiker und Fotografen auf einfache Weise Nutzungsrechte an ihren selbst erstellen Werken einräumen konnten.[85] Bei den CC-Lizenzen handelt es sich um allgemeine Geschäftsbedingungen (AGB), die Nutzer „vor“ dem Erwerb des E-Books kennen müssen.

Die CC-Rechtemodule

Die CC-Lizenz besteht aus drei Lagen. Die erste Lage ist der Lizenzvertrag (Legal Code), der rechtlich maßgeblich und gerichtsfest und den nationalen Rechtsordnungen angepasst ist. Die zweite Lage ist eine Kurzversion des Lizenzvertrages, die Lizenzurkunde (Commons Deed). Diese sollte jeder Laie verstehen. Die dritte Lage besteht aus den sogenannten Metadaten zum Werk und sollte von den Suchmaschinen gefunden werden. Das CC-Icon (bzw. ein Textlink auf die Lizenz) zeigt an, dass der Text, das Foto oder das Video unter der CC-Lizenz und unter welcher Version der CC-Lizenz steht.

Der Urheber kann über 4 Module regeln, wie andere das Werk nutzen dürfen. Die einzelnen Module setzen sich aus 2-Buchstaben-Kürzeln zusammen, welche die Rechte und Pflichten der Lizenznehmer festlegen.

Kürzel	Bedeutung	Kurzerklärung
BY	Namensnennung (Attribution)	Pflicht zur Nennung des Urhebers CC-Nennung und Link zur Lizenz
NC	Nicht kommerziell (Non-Commercial)	Das Werk darf nicht kommerziell genutzt werden.
ND	keine Bearbeitungen (No Derivatives)	Das Werk darf nicht bearbeitet werden.
SA	Weitergabe nur unter derselben Lizenz (Share Alike)	Das Werk muss auch nach der Bearbeitung wieder unter der gleichen Lizenz veröffentlicht werden (Copyleft-Prinzip)

Tab. 06: Die CC-Rechtemodule

84 „GNU General Public License“. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 7. Juni 2015, 11:10 UTC. URL: http://de.wikipedia.org/w/index.php?title=GNU_General_Public_License&oldid=142868555 (Abgerufen: 11. Juni 2015, 16:49 UTC)

85 „Creative Commons“. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 9. Juni 2015, 06:44 UTC. URL: http://de.wikipedia.org/w/index.php?title=Creative_Commons&oldid=142925701 (Abgerufen: 11. Juni 2015, 16:50 UTC)

Anbieter von CC-Inhalten

Urheber, die ihre Werke unter die CC-Lizenz stellen wollen, müssen vorab klären, ob diese überhaupt unter die CC-Lizenz gestellt werden können. Für Software gibt es eigene Lizenzen. Voraussetzung für CC-Inhalte ist, dass der Urheber das alleinige Nutzungsrecht am Werk innehat. Sind mehrere Urheber Inhaber des Urheberrechts, müssen alle mit der CC-Lizenz einverstanden sein. Die Entscheidung, CC-Inhalte zu veröffentlichen, ist unwiderruflich – andernfalls gäbe es für Nutzer keine Rechtssicherheit, CC-lizenzierte Inhalte dauerhaft zu nutzen. Die CC-Schutzdauer erlischt, so wie die urheberrechtliche Schutzdauer, 70 Jahre nach dem Tod des Urhebers.

Die CC-Lizenz ist modular aufgebaut. Der Urheber kann nach dem Baukastenprinzip eine Lizenz zusammenstellen, die am besten seinen Interessen entspricht. Aus der Kombination der vier Rechtemodule ergeben sich sechs Kernlizenzen.[86]

Icons	Kürzel	Erklärung	Lizenzbedingungen (Italien)[87]
	BY	Namensnennung	Version 3.0
	BY-NC	Namensnennung nicht kommerziell	Version 3.0
	BY-SA	Namensnennung Weitergabe unter gleichen Bedingungen	Version 3.0
	BY-NC-SA	Namensnennung nicht kommerziell Weitergabe unter gleichen Bedingungen	Version 3.0
	BY-NC-ND	Namensnennung nicht kommerziell keine Bearbeitung	Version 3.0
	BY–ND	Namensnennung keine Bearbeitung	Version 3.0

Tab. 07: Die sechs Kernlizenzen

86 http://creativecommons.it/Licenze
87 Die Standardlizenzen der Creative Commons werden weiter entwickelt. Der Stand der Entwicklung kommt als Version zum Ausdruck: http://creativecommons.it/Licenze. CC-Lizenzen der neuen Version 4.0: https://creativecommons.org/licenses/by/4.0/legalcode

Welchen Lizenztyp sollte der Urheber auswählen? Das einfachste Rechtemodul verlangt vom Nutzer nur die Namensnennung des Urhebers, alles andere ist freigegeben. Grundfragen sind, ob man die kommerzielle Nutzung zulassen will oder nicht, ob man Bearbeitungen erlauben will oder nicht und ob die bearbeiteten Inhalte unter gleichen Lizenzbedingungen weitergegeben werden dürfen oder nicht. Ein Autor könnte beispielsweise seine Texte freigeben, aber nicht wollen, dass Verlage seine Texte verkaufen, ohne dass er am Erlös beteiligt ist und dass die Texte von anderen nicht bearbeitet werden dürfen. Die CC-Lizenz des Autors sähe dann so aus: „Vorname, Nachname, CC BY-NC-SA 3.0“ und einem Link auf die entsprechende Lizenz bei creativecommons.org.[88] Die Creative-Commons-Organisation bietet auch einen Generator, mit dem etwa Fotografen die passende CC-Lizenz für den eigenen Weblog zurechtklicken können.[89] Bei Fotos, MP3-Dateien oder Videos wird die gewählte CC-Lizenz den Inhalten in Form von Meta-Daten mitgegeben. So können Nutzer und Suchmaschinen genau sehen, was sie mit dem Inhalt machen dürfen und was nicht.

CC-Lizenzen erlauben dem Urheber trotzdem mit Nutzern eine gesonderte Vereinbarung zu treffen, die zusätzliche Freiheiten ermöglicht. Ein Musiker, der seinen neuen Titel unter der CC-Lizenz CC BY-ND ins Netz stellt, kann einem anfragenden DJ erlauben, seinen neuen Titel zu remixen.

Nutzer von CC-Inhalten

Nutzer oder Kreative, die CC-lizenzierte Inhalte verwenden wollen, stehen vor der Frage, welche Kernlizenz für ihr Vorhaben die passende ist. CC BY-Vorgaben gewähren maximale Freiheiten, denn man muss lediglich den Namen des Schöpfers sowie die Art der Lizenz benennen. Du bist also auf der sicheren Seite, wenn du für deinen Weblog nach CC BY-Fotos suchst.

Eine zentrale rechtliche Frage für Nutzer ist, was kommerzielle Nutzung genau heißt. Bei geschäftlichen Webseiten, die Produkte und Dienstleistungen verkaufen oder bewerben, bestehen keine Zweifel. Will man den rein privaten Weblog mit fremden Landschaftsbildern verschönern, liegt keine geschäftliche Nutzung der Fotos vor. Blogger, die hingegen über Werbebanner Serverkosten refinanzieren wollen, könnten CC-Recht verletzen. Nutzer sollten im Zweifel CC-Inhalte nutzen, die ausdrücklich eine kommerzielle Nutzung erlauben oder den Urheber des Werkes kontaktieren, um zu klären, was man mit dem Werk darf und was nicht.

88 Bei Fotos, MP3-Dateien oder Videos wird die gewählte CC-Lizenz den Inhalten als Meta-Daten mitgegeben, sodass Nutzer weltweit erkennen, was sie mit den Inhalten machen dürfen und was nicht.
89 https://creativecommons.org/choose/

Anbieter/Vermittler	Webadresse	Besonderheiten
Creative Commons	http://search.creativecommons.org	CC-Search greift auf die Suchfunktionen anderer Suchdienste zu, wie Google Images oder Europeana. Nutzer können auswählen, ob sie die Inhalte auch kommerziell nutzen und/oder verändern dürfen.
Google	https://www.google.de	Mit der Suchmaschine Google können Nutzer über die *Erweiterte Suche* (Zahnrad) gezielt nach Inhalten mit den gewünschten Nutzungsrechten suchen.
Flickr	https://www.flickr.com/creativecommons	Die Fotocommunity Flickr bietet eine Vielzahl freier Fotos an. Umfangreichere Suchergebnisse lassen sich über englische Stichworte erzielen.
The Public Domain Review	http://publicdomainreview.org/	The Public Domain Review ist ein Projekt der Open Knowledge Foundation, das jährlich die Werke zusammenstellt, die gemeinfrei wurden.
Wikipedia	https://de.wikipedia.org	Wikipedia bietet Texte unter der CC-Lizenz an; die Rechte für eingebundene Bilder und Videos können durch Anklicken ermittelt werden.
YouTube	http://www.youtube.com	YouTube bietet auch freie Werke an; dafür geben die Nutzer beim Videoportal in die Suchleiste den Suchbegriff ein, gefolgt von einem Komma und „creative commons“.

Tab. 08: Suche nach freien Werken

2.1.4 Rechtsrahmen der Medienwerkstatt

Wir können nun unsere eigene Medienwerkstatt eröffnen, ohne befürchten zu müssen, Ärger mit dem Urheberrecht zu bekommen. In diesem Abschnitt gehen wir kurz die Besonderheiten an, die bei einer Medienproduktion mit Text-, Foto-, Musik-, Audio- und Videowerken auftreten können.

Zustimmungsfrei ist die sogenannte freie Benutzung fremder Werke. Jeder kann sich von der Idee anderer Werke inspirieren lassen und der Idee einen neuen Ausdruck geben. Allerdings müssen dabei die charakteristischen Züge des alten Werkes hinter denen des neuen Werkes verschwinden. Die Unterscheidung zwischen erlaubter freier Benutzung und unerlaubtem Plagiat ist im Einzelfall mitunter schwierig. Denn die kreati-

ven Leistungen fallen sprichwörtlich nicht vom Himmel, sondern bauen auf Ideen anderer auf. Ein Gleichnis besagt: „Wir können deshalb so weit sehen, weil wir auf den Schultern von Riesen stehen.“[90]

Als Beispiel für die anstehenden Rechtsfragen wählen wir ein Weblog.[91] Blogger verwenden für ihre Beiträge Zitate, setzen Links, veröffentlichen Interviews und stellen Fotos sowie Videos zum Interview ein. Dabei kommen sie unweigerlich mit Rechtsfragen in Berührung. Deshalb sollten sie wissen, was in der Medienwerkstatt erlaubt oder verboten ist und wie sie sich durch Lizenzen absichern können.

2.1.4.1 Texte

Du kannst ohne Bedenken in deinem Weblog Zitate verwenden, sofern sie der geistigen Auseinandersetzung dienen. Wichtig beim Zitat ist, dass du den Autor nennst und die Quelle angibst, wo der Artikel erschienen ist (vgl. Zitierregeln). Das Verlinken ist ebenso erlaubt, weil Links bereits als solche eine Quellenangabe darstellen.

Interviews müssen vor der Veröffentlichung vom Befragten autorisiert werden. Zur Dokumentation solltest du das Interview mit einem Aufnahmegerät mitschneiden. Besteht der Befragte auf Vertraulichkeit, darf die Aussage nicht mitgeschnitten und auch nicht zitiert werden. Heimliche Mitschnitte von Gesprächen sind strafrechtlich verboten. Willst du ein Interview veröffentlichen, sind neben den rechtlichen Aspekten auch Regeln journalistischer Art zu beachten.

90 „Zwerge auf den Schultern von Riesen“. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 27. Dezember 2014, 12:46 UTC. URL: http://de.wikipedia.org/w/index.php?title=Zwerge_auf_den_Schultern_von_Riesen&oldid=137147722 (Abgerufen: 11. Juni 2015, 16:52 UTC)

91 Ein Weblog kannst du mit der weltweit bekannten Freeware WordPress betreiben. WordPress ist ein Open-Source-Programm, mit dem du Texte, Fotos, Videos, Audios und Kommentare auf deinem Blog einbinden kannst. Den Nutzern kannst du unterschiedliche Rechte zuweisen. Auf der Webseite des Entwicklers gibt es Hilfen für die Installation und den Betrieb: https://wordpress.org/

Interview-Regeln

1. **Vorabrecherche betreiben**
   Informiere dich vor dem Interview über das Sachthema der Befragung und über deinen Gesprächspartner. Gehst du als Bürgerjournalist gut vorbereitet ins Interview, bist du im Interview selbstbewusster und es besteht die Chance, dass ein interessantes Gespräch zustande kommt.

2. **Gesprächspartner begrüßen**
   Stelle dich mit Namen vor und erkläre deinem Gesprächspartner Ziel und Thema der Befragung und wo du das Interview veröffentlichen willst. Führe erst mal einen kurzen Small Talk mit dem Interviewpartner, dann beginnt das Gespräch nicht so steif. Zu Beginn des Interviews sollten die Namen des Befragten und des Interviewers genannt und Ort, Datum, Zeit sowie Thema der Befragung angegeben werden.

3. **Offene Fragen stellen**
   Stelle offene Fragen, dann kann dein Gesprächspartner nicht einfach nur mit Ja und Nein antworten. Stelle die journalistischen W-Fragen: Wer (Um wen geht es?), Was (ist passiert?), Wann (ist das Ereignis passiert?), Wo (ist etwas geschehen?), Wie (ist das Ereignis passiert?) und Warum (ist das Ereignis passiert?). Überlege bei der Vorbereitung des Interviews, welche Informationen du vom Befragten brauchst, welches der rote Faden des Gesprächs sein soll.

4. **Hilfe nutzen**
   Erstelle eine Liste mit Fragen oder Stichworten auf einem Zettel oder Kärtchen. Das gibt dir Sicherheit, denn solltest du einmal nicht mehr weiterwissen, dann kannst du kurz einen Blick auf deinen Notizzettel werfen.

5. **Kritisch und neugierig sein**
   Höre dem Interviewpartner gut zu. Oft ergeben sich aus dem Interview weitere Fragen. Hake nach, wenn die Antwort ungenau oder oberflächlich ausgefallen ist. Als journalistischer Blogger darfst du weder deine Meinung zu einem Thema in den Mittelpunkt stellen, noch für den Gesprächspartner aus dem Interview eine PR-Maßnahme machen. Ein gutes Interview lebt vom Pro und Contra, deshalb solltest du anwaltlich die Gegenposition des Befragten vertreten.

6. **Keine Frageketten wählen**
   Bilde keine Frageketten, falls der Interviewpartner nicht sofort auf deine Frage antwortet. Bei Frageketten kann dein Gesprächspartner die schwierigen Fragen einfach überhören. Stelle dieselbe Frage in abgewandelter Form; so kann dein Gegenüber überlegen, besser formulieren oder gibt dir die Information, die du gerne hättest.

7. **Interview redigieren**
   In der Regel sprechen die Interviewpartner nicht druckreif, verwenden Wiederholungen, versprechen sich, reden im Dialekt oder begehen Grammatikfehler. Du darfst das Interview sprachlich „behutsam“ glätten, Wiederholungen streichen und unwichtige Antworten weglassen. Der Kern einer Aussage aber darf durchs Redigieren nicht verfälscht werden.

8. **Interview aufbereiten**
   Das Interview muss vor der Veröffentlichung noch journalistisch aufbereitet werden. Wähle eine Titelüberschrift, die neugierig macht, das Interview zu lesen. Verfasse einen Vorspann, der den Internetnutzer über den Inhalt des Interview informiert. Längere Interviews kannst du auch in Abschnitte gliedern und als Abschnittsüberschriften kannst du zugespitzte Formulierungen des Befragten wählen.

9. **Interview autorisieren**
   Lege das Interview vor der Veröffentlichung dem Befragten zur Genehmigung vor. Das kann dazu führen, dass der Befragte Sätze streicht oder umschreibt. Schicke deinem Interviewpartner den reinen Interviewtext ohne Titel und Vorspann zur Autorisierung, so gibst du ihm keinen Anlass für Abänderungswünsche. Wähle als Datenformat nicht das Word-, sondern das PDF-Format. Word-Dokumente laden nämlich dazu ein, am Text herumzufeilen. Räume dem Befragten eine angemessene Frist zur Autorisierung ein; ist sie abgelaufen, dann kannst du das Interview als freigegeben betrachten.

2.1.4.2 Fotos

Du möchtest den Blog mit Fotos aufhübschen, die du selbst geknipst oder von einer Fotoagentur erworben hast. Welche rechtlichen Aspekte sind hierbei zu beachten? Bei Fotos muss man grundsätzlich zwischen den Rechten des Fotografierten und denen des Fotografen unterscheiden.

Rechte des Fotografierten

Du darfst grundsätzlich Personen nur mit ihrer Zustimmung fotografieren und auf deinem Blog veröffentlichen. Ohne Einwilligung darfst du nur Bildnisse von Personen der Zeitgeschichte, wie Politikern, bekannten Schriftstellern und Wissenschaftlern oder Spitzensportlern ins Netz stellen. Ein Foto der glücklichen Lottogewinnerin, die gerade dabei ist ihren Gewinn von 1 Million Euro von der Lottostelle abzuholen, wäre auch kein Problem, weil hier das öffentliche Interesse an der Berichterstattung überwiegt. Ebenso ungefragt kannst du Personen fotografieren, die nur als Beiwerk einer Sehenswürdigkeit aufscheinen, etwa Spaziergänger, die neben einem historischen Gasthaus stehen. Die Personen dürfen jedoch nur eine beiläufi-

Foto 3: Pausenhof OSZ Mals Juni 2013

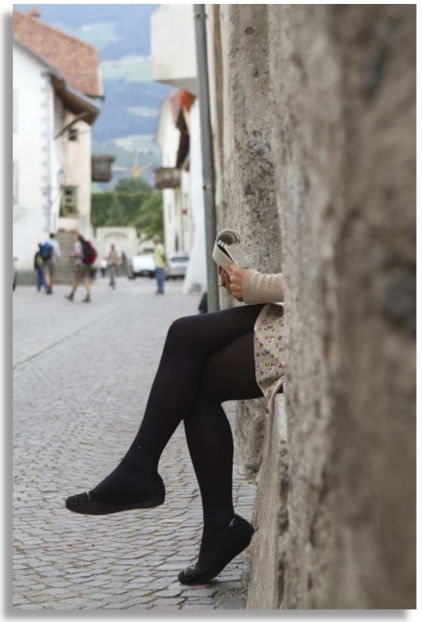


Foto 4: Frau mit Block, Glurns Juli 2011

ge Rolle neben der Sehenswürdigkeit spielen. Dasselbe gilt für Demonstrationen, Sportfesten oder Wochenmärkten, bei denen die Menschenmenge im Mittelpunkt des Fotomotivs steht (vgl. Foto 3). Nicht erlaubt ist etwa, per Teleobjektiv eine einzelne Person aus der Menschenmenge herauszustellen, sodass sie als Person klar erkennbar ist. Unproblematisch sind Personenfotos, wenn die Person als solche nicht erkennbar ist (vgl. Foto 4). Ist die Person klar erkennbar, muss du ihre Zustimmung einholen oder ihr Gesicht verpixeln.

Rechte des Fotografen

Welche Rechte stehen dir als Fotografen zu? Beinahe jedes Foto ist geschützt, unabhängig davon, ob es künstlerisch wertvoll ist oder nur eine geringe künstlerische Qualität aufweist, wie die sogenannten Knipsbilder. Schutzlos sind Fotos, denen jegliche Kreativität fehlt, wie Fotos mit Notebook-Kameras oder Blitzer-Fotos aus einer Verkehrsüberwachung. Zu den wichtigsten Rechten des Fotografen zählen das Urheberpersönlichkeitsrecht und das Verwertungsrecht.

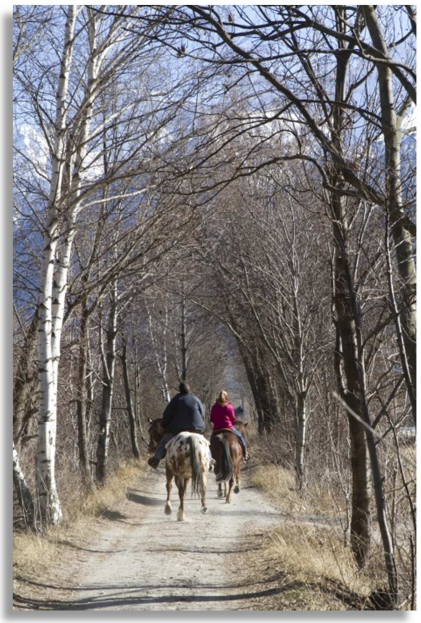


Foto 5: unbearbeitetes Foto

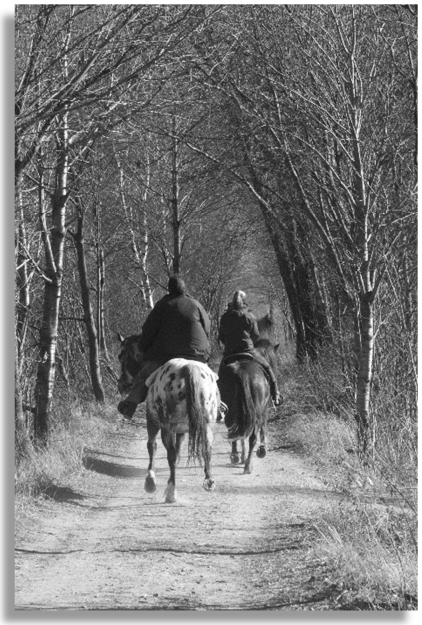


Foto 6: bearbeitetes Foto für Schwarzweiß-Zeitung

Das Urheberpersönlichkeitsrecht sieht u. a. vor, dass der Fotograf gegen die Veröffentlichung eines bearbeiteten Fotos vorgehen kann. Mithilfe von Bildbearbeitungsprogrammen kann man nämlich Fotos beschneiden, die Belichtung, den Kontrast, die Temperatur korrigieren oder Falten retuschieren und Zähne blanchieren. Für den Fotografen stellt sich die Frage, wo die Grenze der eigenmächtigen Bearbeitung durch die Nutzer liegt. Der Lizenznehmer darf Änderungen des Fotos vornehmen, die für dessen Nutzung erforderlich sind. So kann ein Foto mit einer Dateigröße von 30 MB im Netz nicht veröffentlicht werden, sondern muss auf eine vertretbare Größe skaliert werden. Ebenso kann in einer Tageszeitung, die noch in Schwarzweiß erscheint, kein Farbfoto veröffentlicht werden (vgl. Foto 5, 6). Ob der Fotograf Eingriffe in sein Werk abwehren kann oder nicht, hängt letztlich nicht vom Urheberrecht, sondern von seiner Marktmacht ab. Nur Starfotografen müssen nicht befürchten, dass sie keine Aufträge mehr erhalten, wenn sie jede Änderung an ihren Lichtbildwerken ablehnen.

Das Verwertungsrecht ermöglicht dem Fotografen zu bestimmen, ob seine Fotos vervielfältigt oder nur in einer bestimmten Weise genutzt werden dürfen. Überträgt der Fotograf die Nutzungsrechte an eine Fotoagentur, schließt er mit der Agentur einen Lizenzvertrag ab. Für dein Weblog bedeutet dies, dass du fremde Fotos nur unter der Lizenz des Fotografen veröffentlichen darfst.

Veröffentliche Fotos mit Angaben zu deiner Person, Datum der Herstellung sowie der Lizenz, unter der das Foto steht. Internetnutzer wissen dann auf Anhieb, was sie mit deinem Foto tun dürfen und was nicht und an wen sie sich bei offenen Fragen wenden müssen. Führst du einen Fotoblog, dann denke auch an die Verschlagwortung der Fotos, sodass Bildersuchmaschinen deine Fotos auch finden. Überlege gut, welche Stichworte (Tags) am ehesten zu dem Foto passen. Fotografierst du einen Feuersalamander, kannst du die Art (Feuersalamander), die regionalen Mundarten (Feuermolch, Erdmolch oder Tattermandl), den wissenschaftlichen Namen (Salamandra salamandra), die Familie (echte Salamander) und die Klasse (Lurche) als Stichworte verwenden.

Tipp

Lass dir eine schriftliche Einwilligungserklärung von den Personen geben, die auf Fotos abgebildet sind, die du im Netz veröffentlichen willst. In der Erklärung sollten der Name der Person, der Verwendungszweck, der Ort, das Datum und die Unterschrift des Abgebildeten aufscheinen.

Lizenzvertrag-Check

1. Für welche Medien darf das Foto verwendet werden? Nur in einem Blog, nicht aber in Foren und nicht auf Facebook?
2. Für welches Land darf das Foto genutzt werden, falls es sich um eine Offline-Nutzung handelt?
3. Erhält der Lizenznehmer ein einfaches oder ein ausschließliches Verwertungsrecht?
4. Darf der Lizenznehmer die Nutzungsrechte seinerseits weiterveräußern?
5. Darf der Lizenznehmer das Foto bearbeiten? Wenn ja, in welchem Umfang?
6. Enthält der Lizenzvertrag eine sogenannte Total-Buy-out-Klausel, also eine pauschale Übertragung sämtlicher Nutzungsrechte am Foto?

Urheberrecht vs. Persönlichkeitsrecht

Urheber- und Persönlichkeitsrechte können bei Bildnissen in Konflikt geraten. So könnte es sein, dass der Fotografierte sein Bildnis, das ein professioneller Fotograf im Auftrag für eine Bewerbung angefertigt hat, nicht auf seine Webseite stellen darf. Das Urheberrecht räumt nämlich dem Fotografen das Recht ein zu entscheiden, ob und wo sein Werk veröffentlicht werden darf. So darf der Fotografierte sein eigenes Bild nur mit Zustimmung des Fotografen im Netz veröffentlichen; andernfalls geht er das Risiko einer kostenpflichtigen Abmahnung ein. Genauso kann es umgekehrt sein. Schießt der Fotograf etwa ein Straßenfoto, auf dem eine Person im Vordergrund klar zu erkennen ist, darf er dieses auch nicht auf seine Webseite hochladen, um damit Werbung als Fotograf zu betreiben. Der Fotograf muss zuvor die Erlaubnis des Fotografierten einholen; dieser hat ein „Recht am eigenen Bild“.

Suchst du für dein Weblog kostenlose Fotos, stellen die bereits angesprochenen freien Lizenzen, wie die CC-Lizenz eine Alternative zu den kostenpflichtigen klassischen Lizenzverträgen dar. Prüfe dabei aber

stets, was die Lizenz konkret erlaubt: Darfst du das Foto auch bearbeiten, darfst du es kommerziell nutzen? Fotografierst du selbst aus reiner Freude oder willst du nichtkommerziellen Webanbietern deine Fotos zur freien Nutzung zur Verfügung stellen, dann kannst du sie auch unter der CC-Lizenz[92] veröffentlichen.

Agentur- und Urhebervermerk

Veröffentlichst du fremde Fotos, auch solche, die unter einer freien Lizenz stehen, musst du einen Urhebervermerk anführen, um später vor teuren Abmahnschreiben gefeit sein. Der Urhebervermerk muss in der Weise erfolgen, dass kein Zweifel an der korrekten Zuordnung des jeweiligen Fotos entstehen kann. Bei Fotos von Fotoagenturen muss neben dem Urheber- auch der Agenturnachweis angeführt werden: *Foto: Agentur – Name* des Fotografen: *Titel, Entstehungsjahr*.

Dürfen Fotos, die unter einer CC-Lizenz stehen, nach Belieben in Blogs, Foren oder auf Fanpages in sozialen Netzwerken gepostet werden? Nein, CC-Lizenzen bewirken keinen rechtsfreien Raum. Wer CC-Fotos nutzen will, muss sich an zwei Regeln halten, nämlich den Namen (oder das Pseudonym) des Fotografen nennen und zur maßgeblichen CC-Lizenz verlinken. Willst du deinen Blog mit Fotos aus Wikipedia bebildern, musst du dich zuvor über deren Nutzungsbedingungen genau informieren. Klicke dazu das gewünschte Foto an, dann öffnet sich die Bildbeschreibungsseite mit einer der CC-Lizenzen. Nicht jede CC-Lizenz ist für deinen Verwendungszweck geeignet. Willst du das Foto auch kommerziell nutzen, dann darf dies nicht untersagt sein. Soll nur ein Ausschnitt des Fotos veröffentlicht werden, dann muss die CC-Lizenz auch die Bearbeitung erlauben. Die Bildbeschreibungsseite gibt den Namen des Fotografen bzw. sein Pseudonym und die Lizenz des Fotos an. Es genügt nicht unter das Foto einfach CC-Lizenz zu schreiben, denn es gibt verschiedene CC-Kernlizenzen. Gib auch die Webadresse der Seite an, auf der das Foto steht. Ein korrekter Urhebervermerk eines Wikipedia-Fotos sieht so aus: Foto: Name des Fotografen

Tipps fürs Fotoporträt

1. **Motiv**
   Zeige mehr als nur das Abbild der Person, versuche die ganze Persönlichkeit einzufangen. Zieht dein Interviewpartner bei einer zentralen Frage skeptisch die Augenbraue nach oben, kann das dessen Haltung zum gesamten Thema des Interviews ausdrücken. Vergiss die Augen nicht, sie sind bei Porträts am wichtigsten. Wähle als Bildstil auf deiner Kamera das Porträt oder überbelichte um eine Blende, dann wirkt das Foto weicher.
2. **Licht**
   Beachte, dass eine direkte Sonneneinstrahlung oder ein Blitz zu harten Schatten und Schlaglichtern führt. Positioniere die Person so, dass ihr die Sonne im Rücken steht, oder wähle eine gedämpfte Lichtquelle; sie bewirkt dezente Schatten. Harte Schatten kannst du auch mit einem Blitz etwas aufhellen.
3. **Bearbeitung**
   Fotos gelingen selten abzugsreif. Prüfe mithilfe deines Bildbearbeitungsprogramms, ob das Foto etwa nachgeschärft, die Belichtung korrigiert oder ob nur ein Ausschnitt veröffentlicht werden sollte, weil Unwichtiges das Fotomotiv nicht stören sollte. Als Letztes muss das Foto noch für das Web optimiert werden. Das heißt, die Bildgröße muss entsprechend verringert werden und die Farben werden standardmäßig auf 256 Farben reduziert.

92 https://creativecommons.org/licenses/

und Link zur CC-Lizenz. *Z. B. Foto[93]: Jörg Hempel,[94] Lizenz: CC BY-SA 3.0 de[95].* Der Urhebervermerk und der Link auf die Lizenz sollten direkt am Foto stehen. Wer den Bildnachweis versteckt anbringt, etwa im Impressum, riskiert auch von Wikipedia-Fotografen eine Abmahnung.

Fotos fürs Internet aufbereiten

Stellst du Fotos ins Netz, dann solltest du zwei Einstellungen beachten, nämlich die der Bildgröße und die der Auflösung (dpi). Für die Bildgröße wird die Einheit Pixel verwendet. Ein Bild auf einer Webseite hat eine maximale Größe von 1024x768 Pixel. Geht die Bildauflösung über die maximale Bildschirmauflösung hinaus, kann das Bild nicht mehr vollständig auf einer Monitorseite angezeigt werden. Die Pixelabmessung kann von Online-Foren vorgegeben sein, sie hängt von der Verwendung des Fotos ab und muss auch zum Layout der Webseite passen. Damit ein Foto im Browser in einer vertretbaren Zeit geladen wird, sollte es die Dateigröße von 300 KB nicht überschreiten. Ladet das Foto zu langsam, klicken sich die Surfer weg. Hat das Original-Foto z. B. eine Dateigröße von 102,5 MB, muss sie erst einmal auf etwa 300 KB des Ziel-Fotos skaliert werden. Die Bilddatei kannst du beispielsweise mit Adobe Photoshop verkleinern.

Anbieter	Webadresse	Besonderheiten
Flickr	https://secure.flickr.com	Flickr ist eine Foto-Plattform, auf die sowohl Amateure als auch professionelle Fotografen ihre Fotos hochladen können. Ihre Nutzer können die Fotos in Galerien sortieren, mit Kommentaren versehen, bestimmten Nutzern den Zugriff auf die eigenen Fotos gewähren und sich von Fotos anderer Fotografen inspirieren lassen.
Pinterest	http://pinterest.com	Pinterest ist ein soziales Netzwerk, in dem Nutzer Fotos, die ihnen im Netz gefallen, an die Pinnwand heften können. Die anderen Nutzer können diese Fotos nur kommentieren oder auch an ihre eigene Pinnwand heften.
Tumblr	https://www.tumblr.com	Tumblr ist eine Foto-Plattform, auf der Fotografen ihre Fotos in einem eigenen Blog veröffentlichen können. Die Fotos sind für alle zugänglich.

Tab. 09: Foto-Communitys im Netz

93 Foto als Textlink zu: https://commons.wikimedia.org/wiki/File:Panaeolus_semiovatus_LC0334.jpg
94 Name des Fotografen als Textlink zu: https://commons.wikimedia.org/wiki/User:LC-de
95 Die Art der CC-Lizenz als Textlink zu: https://creativecommons.org/licenses/by-sa/3.0/de/deed.en

Bilder skalieren

Starte Photosphop, öffne das Bild und gehe über den Menüpunkt *Bild* zu *Bildgröße…*. Im Dialog-Fenster *Bildgröße* (Abb. 10) kannst du die Anzahl der Pixel, Dateigröße und Größe des Bildes passgenau verringern. Mit Gimp[96] oder Down-Sizer,[97] das sind kostenlose Alternativen zu Photoshop, kannst du ebenso Bilder fürs Web optimieren.

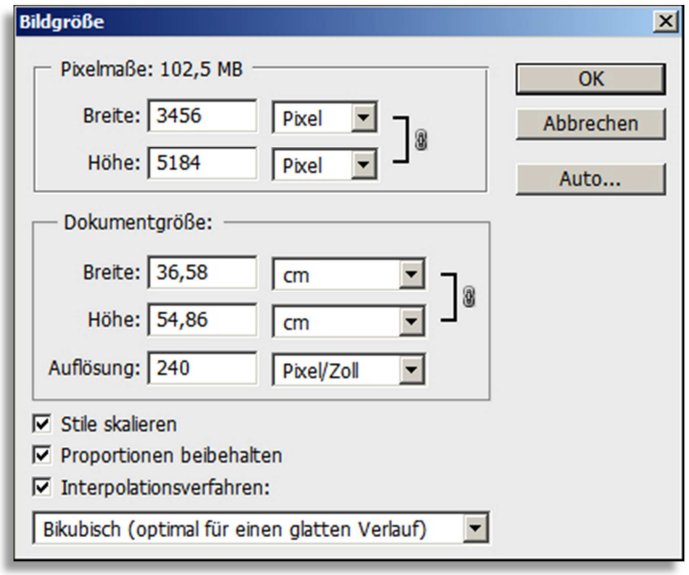


Abb. 10: Original Pixelmaße

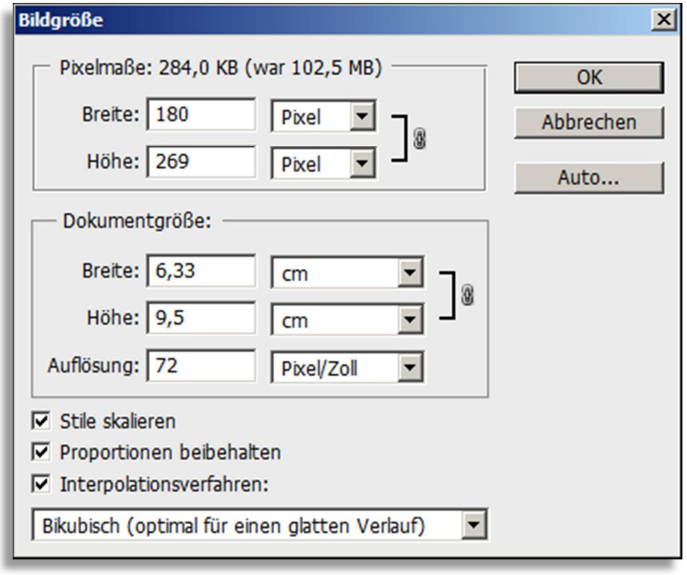


Abb. 11: Skalierte Pixelmaße

Speichere die Fotos, die fürs Internet vorgesehen sind, mit einer Auflösung von 72 dpi. Dies bedeutet, dass 72 Bildpunkte pro Zoll (=2,54 cm) angezeigt werden. Die Größe des Bildes hängt von Pixelanzahl und Bildschirmauflösung ab. So wird ein Bild mit 180 Pixeln Breite und 72 dpi Auflösung auf einem Monitor mit 72 Pixeln pro Zoll mit einer Breite von 6,35 cm angezeigt [(180 : 72) x 2,54 = 6,35 cm] (Abb. 11). Willst du das Foto bei gleicher Auflösung verkleinern, musst du die Anzahl der Pixel entsprechend verringern. Soll das Bild hingegen über die Originalgröße hinaus vergrößert werden, leidet die Bildqualität. Die neuen Pixel werden hierbei aus den vorhandenen Pixeln errechnet. Wo keine zusätzlichen Details auf dem Bild zu sehen sind, können durch die zusätzlichen Pixel auch keine erfunden werden. Das Bild kann so unschärfer werden.

96 http://www.gimp.org/
97 http://breakoutbox.de/software/software.html#downsizer

2.1.4.3 Videos

Du möchtest von einem Interview in einem Café ein Video drehen und auf dein Weblog hochladen. Bevor du einfach mal „drauf losfilmst“, solltest du dir einen Überblick über die rechtliche Situation verschaffen.

Zunächst darfst du nicht einfach Menschen ohne ihre Genehmigung filmen. Lass dir zur Rechtssicherheit eine schriftliche Einverständniserklärung geben, in der der Name und die Adresse des Gefilmten, der Verwendungszweck (Reportage, Werbung, Image) und die Art der Verbreitung (Internet, TV, DVD) angegeben werden. Politiker, Musik-, Film- oder Sportstars dürfen nur bei öffentlichen Anlässen ungefragt gefilmt werden, nicht aber in ihren Arbeitszimmern oder im privaten Bereich.

In privaten Orten gilt das Hausrecht. Das bedeutet, der Inhaber der Privatwohnung, des Cafés oder des Geschäfts bestimmt, ob du filmen darfst oder nicht. In deinem Fall brauchst du also die Drehgenehmigung vom Café-Inhaber.

Gilt für das Videoportal YouTube eine Sonderregelung? Nein, das Urheberrecht gilt auch für YouTube. Du darfst also nur solche Videoclips auf YouTube hochladen, die du selbst gedreht hast. Sind Personen auf dem Videoclip zu sehen, musst du deren Zustimmung einholen. Spielen auf deinem Geburtstagsvideo deine Freunde ein Musikstück, zu dem sie keine Lizenz erworben haben, dann verletzen sie Urheberrecht. Lädst du fremdes Videomaterial auf YouTube hoch, z. B. eine Szene aus einem kommerziellen Video, kann das zur Löschung des YouTube-Channels und zu teuren Abmahnungen führen.

Videorechte-Check

1. Hast du die Rechte am Drehbuch erworben?
2. Hast du eine Lizenz an der Hintergrundmusik, die im Video gespielt wird?
3. Hast du die Rechte der Schauspieler erworben?
4. Hast du die Rechte geklärt, falls im Video ein Kunstwerk, eine Designvase oder ein Notenblatt klar zu sehen ist?
5. Hast du die Fotografierten gefragt, ob ihr Bildnis fürs Video genutzt werden darf?
6. Hast du eine Lizenz am fremden Filmmaterial, falls du mehr als eine einzelne Filmsequenz zitieren willst?
7. Hast du eine Drehgenehmigung vom Gebäudeinhaber, falls du Videosequenzen im Gebäude drehen möchtest?
8. Hast du die Drehgenehmigung vom Konzertveranstalter? Ist die private Videoaufnahme erlaubt? Was steht hierzu auf der Webseite des Veranstalters oder auf der Rückseite der Eintrittskarte?

2.1.4.4 Audios

Du brauchst Musik für dein Interview, das du als Podcast auf deinem Weblog anbieten möchtest. Willst du Ärger vermeiden, musst du dich um die Musikrechte kümmern. Jede Musik ist grundsätzlich urheberrechtlich geschützt und darf nicht ohne Lizenz genutzt werden.

Die Lizenzfrage ist keine einfache, weil sich das Musikwerk aus mehreren Einzelleistungen zusammensetzt, die jeweils mit eigenen Rechten verknüpft sind. Der Komponist schafft eine Klangfolge, die das Musikwerk bildet und urheberrechtlich geschützt ist. Geschützt ist auch der Songtext, der urheberrechtlich ein Sprachwerk ist. Nun kommt die Leistung der Musiker hinzu, die die Musik spielen und als Werkinterpreten bezeichnet werden. Die Leistung der Musiker wird durch das Leistungsschutzrecht geschützt. Hinzu kommt noch ein weiteres Leistungsschutzrecht, nämlich das Recht der Plattenfirma, die die Rechte am Tonträger, beispielsweise an der CD erwirbt. Brauchst du also Musik für dein Weblog, wäre im Prinzip eine ganze Reihe von Lizenzen zu erwerben. In der Regel übertragen aber die Komponisten, Texter und Interpreten die Urheber- und Leistungsschutzrechte an einen Musikverlag oder eine Plattenfirma, die für die Vermarktung des Musikwerkes sorgt.

Bei Musikwerken müssen also zwei Rechte unterschieden und erworben werden, das Verlagsrecht (Publishing Right) und das Masterrecht (Masterright). Das Verlagsrecht ist das Nutzungsrecht an der Musik, das in der Regel die Musikverlage verwalten und erst 70 Jahre nach dem Tod des Künstlers erlischt. Das Masterrecht hingegen ist das Leistungsschutzrecht (Tonträgerrecht) an der Musikaufnahme und erlischt 50 Jahre ab dem Datum ihrer Aufnahme.

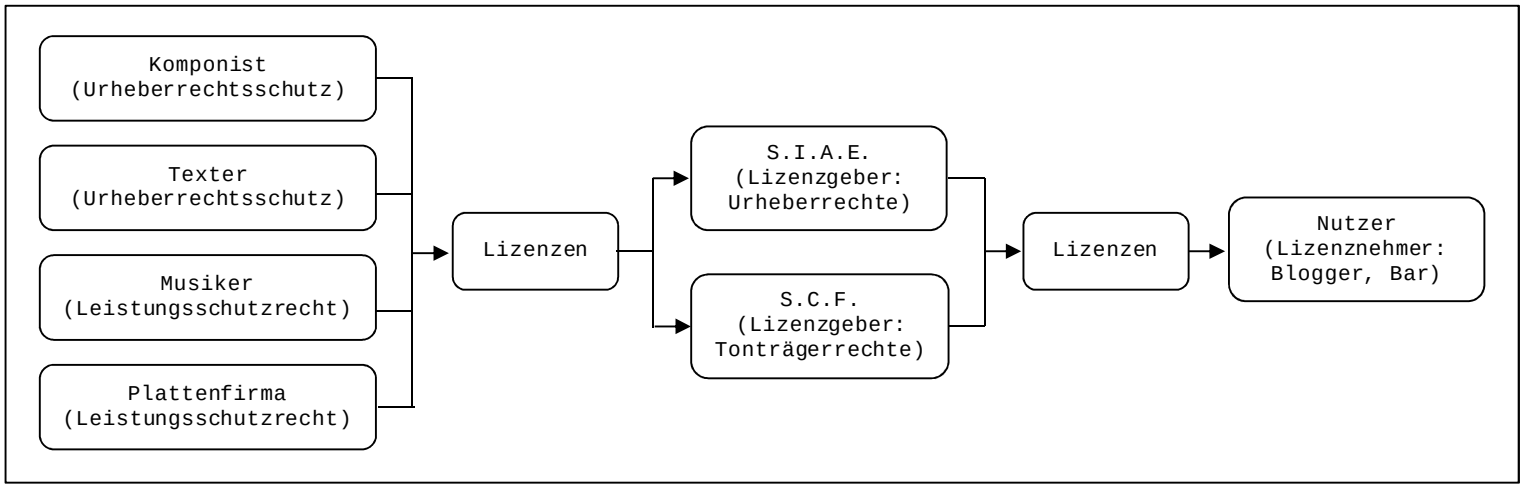


Abb. 12: Lizenz von Verwertungsgesellschaften

In Italien sind die Lizenzanfragen für Musik in der Praxis an die beiden Verwertungsgesellschaften S.I.A.E.[98] (Società Italiana degli Autori ed Editori) und S.C.F.[99] (Società Consortile Fonografici per azioni) zu stellen; sie vertreten die Rechte der Künstler, Verlage und Tonträger. Du gehst hierbei nur eine Vertragsbeziehung mit der Verwertungsgesellschaft ein und nicht mit den einzelnen Urhebern (vgl. Abb. 12). Lizenzierung bedeutet, dass du ein geschütztes Musikwerk nutzen darfst, etwa zur Vertonung eines Podcasts, der auf einem nichtkommerziellen Weblog für die Dauer von 10 Jahren angeboten wird.[100]

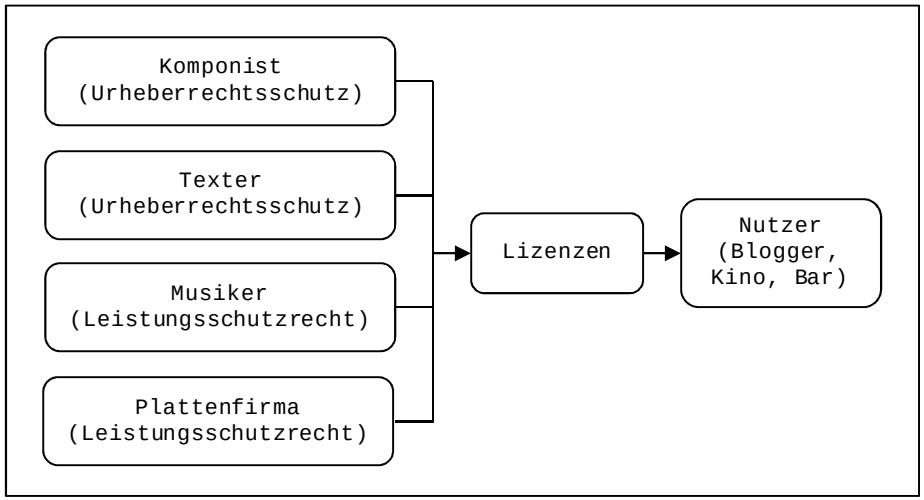


Abb. 13: Lizenz von Urheber, Musiker und Plattenfirma

Willst du ausschließlich selbst produzierte Audiodateien als Podcast anbieten, bist du alleiniger Urheber und musst niemanden um Erlaubnis (Lizenz) fragen. Das ist dann der Fall, wenn du deine eigenen Blogbeiträge vorliest und als MP3-Dateien zum Herunterladen anbietest, z. B. als Service für Blinde oder für Leute, die das „Radio zum Mitnehmen“ schätzen. Als Produzent von Podcasts steht dir das Recht zu, alleine darüber zu entscheiden, ob die Podcasts verbreitet werden dürfen oder nicht. Gibst du dein Podcast frei, solltest du nicht vergessen festzulegen, wie die Audiodatei genutzt werden darf. Du kannst beispielsweise bestimmen, dass dein Podcast nur privat kopiert und verbreitet werden darf und für eine kommerzielle Nutzung deine ausdrückliche Zustimmung erforderlich ist. Eine einfache Möglichkeit hierzu liefert die Creative Commons-Lizenz an, mit deren Hilfe du nach dem Baukastenprinzip eine passende Lizenz zusammenstellen kannst.[101]

Es gibt Musikarchive im Netz, die „freie Musik“ mit Creative Commons-Lizenzen anbieten, die standardmäßig eine kostenlose Nutzung für nichtkommerzielle Zwecke ermöglichen. Ein Blick auf die Musik-Communities wie

98 www.siae.it/; lokale Büros der SIAE: http://www.siae.it/SIAE_InItalia.asp
99 http://www.scfitalia.it
100 Die S.I.A.E. stellt eine Datenbank zur Verfügung, in der du nach Musiktiteln recherchieren kannst: http://operemusicali.siae.it/OpereMusicali/start.do?language=it
101 https://creativecommons.org/licenses/

Archive.org[102], Free Music Archive[103] oder dig.ccmixter[104] lohnt. Eine Alternative könnten auch die sogenannten Netzlabels sein, die kostenlose MP3 zum Download anbieten.[105]

2.1.4.5 Online-Schülerzeitung

Für die Medienwerkstatt kann eine Online-Schülerzeitung durchaus reizvoll sein. Sie kann die Kommunikation zwischen Schülern verbessern, ihre Meinungsbildung fördern und ihnen ermöglichen, ihr Können als Texter, Fotograf, Grafiker und Layouter unter Beweis zu stellen. Viele Fragen müssen bei so einem Projekt geklärt werden, wie Ausrichtung der Schülerzeitung, Ablauf der Redaktionsarbeit, Layout oder welche journalistischen Stilformen gewählt werden sollen. In jedem Fall sollen sich die Schüler-Redakteure im Vorfeld mit den rechtlichen Rahmenbedingungen einer Online-Schülerzeitung vertraut machen, wollen sie rechtliche Auseinandersetzung vermeiden. Anwaltliche Abmahnungen gehören zwar nicht zum Alltag einer Schülerzeitung, die Schüler-Journalisten sollten aber wissen, wann sie Gefahr laufen, ein juristisches Minenfeld zu betreten.

Grundrecht auf Meinungs- und Pressefreiheit

Zuallererst ist jedoch klarzustellen, dass die Meinungs- und Pressefreiheit ausdrücklich in der italienischen Verfassung verankert ist und somit „Verfassungsrang“ hat. Die Meinungsfreiheit beinhaltet das Recht, sich eine eigene Meinung zu bilden, diese frei zu äußeren und durch „Wort, Schrift und jedes andere Mittel“ zu verbreiten. Unter „jedes andere Mittel“ fällt auch die Verbreitung über das Internet. Ausgestaltung und Grenzen der Meinungs- und Pressefreiheit regeln Gesetze. Was fällt aber alles unter den Begriff „Meinung“? Darunter versteht man eine wertende Aussage, eigene Einschätzungen und Beurteilungen des Autors. Es gibt keine „richtigen“ oder „falschen“ Meinungen. Die Meinungsfreiheit schützt die geistige Auseinandersetzung in demokratisch verfassten Gesellschaften. Im Namen der Meinungsfreiheit ist freilich nicht alles erlaubt. Eingriffe in die Meinungs- und Pressefreiheit dienen dem Schutz anderer wichtiger Rechtsgüter. So sind die Beleidigung (Art. 595 c.p.), die üble Nachrede (Art. 595 c.p.) oder die Verun-

Art. 21 Verf.

„(1) Jedermann hat das Recht, die eigenen Gedanken durch Wort, Schrift und jedes andere Mittel der Verbreitung frei zu äußern.
(2) Die Presse darf weder einer behördlichen Ermächtigung noch einer Zensur unterworfen werden.“

102 www.archive.org
103 http://freemusicarchive.org
104 http://dig.ccmixter.org
105 Internetarchive Netlabels: http://www.archive.org/details/netlabels

glimpfung der Republik verboten. Ungesetzlich ist beispielsweise auch die Aufforderung zum Gesetzesungehorsam, etwa die Steuern nicht zu bezahlen (Artt. 414 ff. c.p.).

Impressumspflichten

Eine Online-Schülerzeitung muss ein Impressum enthalten. Werden strafbare Inhalte veröffentlicht, kann der Staatsanwalt aus dem Impressum ersehen, wer für den Inhalt zur Verantwortung gezogen werden kann. Will ein Leser falsche Tatsachen richtigstellen, weiß er, wohin er die Gegendarstellung senden kann. Das Impressum muss den Namen, Vornamen und die Anschrift des verantwortlichen Redakteurs anführen. Name und Anschrift der Druckerei entfallen bei einer Online-Zeitung.

Gegendarstellungsrecht

Zum Schutz der Bürger vor der Macht der Medien sieht das Pressegesetz ein „Recht auf Gegendarstellung" vor. Anspruch auf Gegendarstellung haben jene Personen, die durch eine Tatsachendarstellung unmittelbar betroffen sind. Der Betroffene erhält durch die Gegendarstellung einen „gleich langen Spieß" wie die Schülerzeitung – Tatsachenbehauptung gegen Tatsachenbehauptung. Die Gegendarstellung muss die beanstandeten Tatsachen bezeichnen, unverzüglich erfolgen und darf sich nur auf tatsächliche Angaben beschränken. Die Schülerredaktion ist also verpflichtet, wenn sie über eine Person berichtet, auch deren Gegendarstellung in der nächsten Online-Ausgabe zu veröffentlichen. Die Gegendarstellung wird durch die Überschrift „Gegendarstellung" als solche gekennzeichnet. Die Schülerredaktion kann der Gegendarstellung auch einen Kommentar hinzufügen, etwa ein Bedauern, falls die Tatsachendarstellung tatsächlich falsch war. Ist die Redaktion aber der Auffassung, dass die Tatsachendarstellung sattelfest ist, kann sie ihren Kommentar auch mit dem Satz ergänzen: „Die Redaktion bleibt bei ihrer Darstellung."

Art. 27 Verf.

„(2) Der Angeklagte wird bis zur endgültigen Verurteilung nicht als schuldig betrachtet."

Pressekodex

Auch Schüler-Journalisten unterliegen dem Pressekodex. Dieser sieht beispielsweise vor, dass Journalisten zur Wahrheit verpflichtet sind. Schüler, die Beiträge für die Online-Zeitung verfassen, sind verpflichtet, die Richtigkeit der Informationen sorgfältig zu überprüfen. Bestehen Zweifel, sollte eine zweite, unabhängige Quelle zu einem Faktencheck herangezogen werden. Auch in Online-Zeitungen muss Werbung als solche gekennzeichnet sein. Der Leser sollte klar erkennen können, welche Inhalte journalistischen Charakter haben und welche den Interessen der Werbewirtschaft dienen. Zur fairen Presse gehört schließlich das Prinzip der Ausgewogenheit. Bei sich widersprechenden Standpunkten, etwa zum Bau eines Windradparks,

dürfen Schüler-Journalisten nicht nur den Standpunkt der Befürworter, sondern müssen auch den der Kritiker wiedergeben.

Urheberecht

Auch eine Online-Schülerzeitung kommt mit dem Urheberrecht in Berührung. Werke wie Texte, Fotos, Audios, Videos oder Grafiken genießen urheberrechtlichen Schutz. Eine Verwendung geschützter Werke außerhalb des privaten Bereichs und außerhalb des Klassenzimmers ist grundsätzlich nur mit Einwilligung der Urheber zulässig. Erstellen die Schüler sämtliche Inhalte der Schülerzeitung selbst, ergeben sich keine urheberrechtlichen Probleme. Schüler müssen in einem solchen Fall weder den Urheber noch die S.I.A.E. um Erlaubnis fragen, ihre Inhalte für die Schülerzeitung nutzen zu dürfen.

In der Praxis nutzen die Schüler für eine Online-Zeitung auch fremde Inhalte, zumal es auch einfach geht per „Copy & Paste“ Fotos, Texte oder Ähnliches in das eigene Angebot einzubauen und dieses dadurch aufzuwerten. Handelt es sich um fremde Inhalte, macht das Urheberrecht keinen Unterschied, ob die fremden Inhalte von der Online-Schülerzeitung oder einem kommerziellen Anbieter genutzt werden. Wer fremde Werke ins Netz stellt, braucht eine Lizenz vom Rechteinhaber, unabhängig davon, ob er mit seinem Online-Angebot Geld verdient oder nicht. Eine Möglichkeit Kosten zu sparen und Rechtskonflikte zu vermeiden besteht für die Schüler-Journalisten darin, nach Inhalten zu suchen, die unter einer der freien Lizenzen stehen.

Für die Online-Schülerzeitung gilt selbstverständlich auch das Zitatrecht. Die Schüler dürfen Texte, Fotos oder Musik nicht in beliebiger Weise zitieren, sondern müssen die Zitatregeln beachten. Das bedeutet, die Schüler müssen Autor und Quelle der Werke anführen und die Werke nur im unbedingt erforderlichen Umfang nutzen (vgl. Zitatregeln).

Das Urheberrecht schützt jeden, der Werke publiziert, d. h., auch eure Online-Zeitung ist urheberrechtlich geschützt. Wollt ihr als Schüler-Journalisten eure Texte oder Fotos unter eine freie Lizenz stellen, solltet ihr dies im Impressum deutlich machen. Diskutiert in der Redaktion, was ihr den Nutzern eurer Zeitung erlauben wollt und was nicht und wählt dann ein entsprechendes Lizenzmodell aus.

Schutz der Informanten und Informationen

Zur Pressefreiheit gehört schließlich, dass die Informanten geschützt sind und dass das Redaktionsgeheimnis gewahrt bleibt. Das Grundrecht auf „freien und geheimen Schriftverkehr“ ist zwar ausdrücklich in der Verfassung vorgesehen (Art. 15), kann aber im Netz ohne technische Hilfsmittel nicht durchgesetzt werden. Cyberkriminelle oder Sicherheitsbehörden können E-Mails wie die vielzitierten Postkarten lesen. Wollt ihr euren E-Mail-Verkehr wirksam vor neugierigen Blicken schützen, ist eine Mail-Verschlüsselung unumgäng-

lich. Damit eure Leser oder Informanten verschlüsselt mit der Redaktion kommunizieren können, müsst ihr den öffentlichen Schlüssel im Impressum zum Download anbieten oder regelmäßig per E-Mail-Anhang verbreiten.[106]

2.2 Der Datenschutz

Wer die Dienste des Internets nutzt, als Konsument oder als Produzent, hinterlässt zwangsläufig Datenspuren. Bei der Einwahl ins Internet entstehen beim Access-Provider Verbindungsdaten, wie zugewiesene IP-Adresse, Datum und Uhrzeit der Einwahl. Daten entstehen bei jeder deiner Suchanfragen. Jedes Mal, wenn du bei Google einen Suchbegriff eingibst, protokolliert Google den eingegebenen Suchbegriff, deine IP-Adresse, den Browsertyp, das verwendete Betriebssystem sowie Datum und Uhrzeit der Suchanfrage. Zudem speichert Google, welche Fundstellen du tatsächlich besucht hast.[107] Rufst du eine Webseite auf, legt der Web-Server eine Log-Datei an und speichert neben IP-Adresse und Access-Provider auch geografische Informationen (Land, Region, Ort des Access-Providers) und Browser Details (Browser, Referer, Cookie). Nutzt du die zahlreichen kostenlosen Dienste wie E-Mails, Chats oder soziale Netzwerke, musst du dich erst registrieren und somit persönliche Daten preisgeben. Werden die Anmeldedaten mit dem Nutzerverhalten verknüpft, käme bereits ein sehr detailliertes Bild über dich zustande. Kennen die Internetfirmen auch die Inhalte deiner E-Mails, über Routenplaner dein Urlaubsziel, über den „Gefällt-mir-Button“ deine Interessen im Internet und über netzwerkfähige Alltagsgeräte dein tägliches Verbraucherverhalten,[108] dann entsteht noch ein präziseres Profil.

Was passiert mit all diesen Daten? Internetfirmen wie Google, Apple, Microsoft und Facebook sammeln all die Daten, um sie „zu verschiedenen Zwecken“ auszuwerten, etwa um Kundenprofile an ihre Werbekunden zu verkaufen, damit diese ihrerseits ihren Kunden individuelle Angebote erstellen können. Teilst du deinen Freunden per E-Mail, SMS oder auf deiner Blog-Webseite mit, dass du reif für einen kurzen Stadturlaub

106 Informationen, wie die Technik der E-Mail-Verschlüsselung funktioniert und wie die Vertraulichkeit der E-Mail-Nachrichten auf dem Smartphone gewährleistet werden kann, findet ihr im Kapitel „Smartphone sicher nutzen“.

107 Wie Google aus Interessensprofilen der Nutzer entsprechende Anzeigen erzeugt und in Google-Suche, in Gmail und im Web einblendet, erklärt Google auf seiner Webseite: https://support.google.com/ads/answer/1634057?rd=1

108 Ein Überblick zu den Alltagsgeräten als Datenspione: Stefan Schmitt (2013): *Ein Bild aus tausend Spuren,* Zeit online, 01.08.2013 – 08:00 Uhr, http://www.zeit.de/2013/32/datenspuren-internet-snowden-prism-tempora. Wissenschaftler der FH Münster haben nachgewiesen, dass sie aus „intelligenten Strommessgeräten“ (Smart Metern) nicht nur ablesen konnten, welche Geräte in der Wohnung genutzt wurden, sondern auch, welches Fernsehprogramm lief sowie ob das Frühstück warm oder kalt zubereitet wurde und ob die Kinder alleine zuhause waren: http://1lab.de/pub/GrJuLo_Smartmeter.pdf

bist, dann bekommst du umgehend Reisangebote.[109] Die „Großen Vier“ sind zurzeit die Verkörperung des Big Data. Die Marktführer versuchen, aus der Informationsflut ihrer Nutzer Profit zu schlagen. Beim Börsengang im Jahr 2012 war die Facebook-Datenbank von mehr als einer Milliarde individueller Profile rund 104 Milliarden Dollar wert. Online-Banken verleihen Geld übers Internet. Die Bonität des Kreditkunden ermitteln sie über schnelle Datenanalysen von Rechenzentren. Dabei spielen der Bildungsstand, das Einkommen und der Wohnort eine Rolle, aber auch welches iPad der Kunde nutzt, eines der Businessklasse oder ein billiges Auslaufmodell und wie häufig er die Löschtaste benutzt. Big Data findet nicht nur in der Geschäftswelt Anwendung. Programme können inzwischen auch Aufsätze von Schülern zuverlässig bewerten.[110]

Warum stellt das Sammeln von Daten eine Gefahr für den Internetnutzer dar? Werden die Datenspuren der Nutzer miteinander verknüpft, ergeben sie ein umfassendes Bild über seine Persönlichkeit. Der Anbieter weiß mehr über den Nutzer als der Nutzer über sich selbst. Es besteht die Gefahr, dass die Bedürfnisse der Nutzer manipuliert werden und dass sie so unüberlegt Artikel kaufen. Gefährdet ist die Privatautonomie. Wie die Privatautonomie im Umfeld des digitalisierten Alltags und der neuen Geschäftsmodelle wirksam geschützt werden kann, ist noch offen.

In diesem Abschnitt zeigen wir den rechtlichen und technischen Schutz der Privatautonomie auf. Der Internetnutzer soll über seine „Bürgerrechte im Netz“ informiert und in der Lage sein, bei seinen Publikationen die Datenspuren zumindest ansatzweise zu managen und zu kontrollieren.

2.2.1 Schutz durch Recht

Das Datenschutzrecht ist ein Grundrecht. Geschützt wird die „informationelle Selbstbestimmung“ der Bürger, die eine Konkretisierung des allgemeinen Persönlichkeitsrechts darstellt (Art. 2 Verf.). Unter „informationeller Selbstbestimmung“ versteht man, dass jeder Einzelne selbst über die Preisgabe und Verwendung seiner persönlichen Daten entscheiden kann. Grundlage für seine Entscheidungen ist der informierte und freie Wille (D.lgs. 196/2003).

Zum Gegenstand der informationellen Selbstbestimmung gehören die personenbezogenen Daten, also alle Informationen über eine bestimmte oder bestimmbare Person. Zu den Personendaten zählen etwa Name, Anschrift, Geburtsdatum, E-Mail-Adresse, Passwörter, PIN, TAN, Fingerabdruck, Röntgenbilder oder Parteizugehörigkeit. Der Datenschutzkodex stellt solche Informationen unter Schutz.

---

109 Jessica E. Lessin u. a. (2012): *Der Kampf der Tech-Titanen geht 2013 weiter,* The Wall Street Journal, 26.12.2012 - 15:43 Uhr, http://www.wsj.de/article/SB10001424127887324669104578202810045851972.html?mg=reno64-wsjde

110 Martin U. Müller u. a. (2013): *Die gesteuerte Zukunft,* in: Der Spiegel 20/2013, S. 64-74.

Personendaten dürfen nur dann erhoben und verarbeitet werden, wenn eine Rechtsnorm dies gestattet oder der Betroffene dazu eingewilligt hat. Dem italienischen Datenschutzkodex liegt die sogenannte Opt-in-Regel zugrunde. Jeder Nutzer muss aktiv werden, um seine privaten Daten freizuschalten, etwa ein Kontrollkästchen aktivieren oder auf einen Button klicken.

> „Zwischen dem Schwachen und dem Starken ist es die Freiheit, die unterdrückt, und das Gesetz, das befreit."
>
> Jean-Jacques Rousseau, Philosoph und Schriftsteller

Einwilligung des Betroffenen

Die Einwilligung darf allerdings nicht „ins Blaue hinein", sondern muss informiert erfolgen. Voraussetzung dafür ist, dass der Einwilligung eine Datenschutzbelehrung vorausgeht, in der in verständlicher Form angeführt wird, welche Daten zu welchem Zweck erhoben werden. Nur so kann der Betroffene tatsächlich erkennen, was mit seinen Daten passiert und eine aufgeklärte und bewusste Entscheidung treffen. Eine bewusste Entscheidung liegt etwa vor, wenn der Betroffene auf ein Kontrollkästchen klicken und sich zuvor durch die Datenschutzbelehrung scrollen muss.

Es dürfen nur solche Daten erhoben werden, die für den angeführten Zweck, etwa für die Abwicklung eines Kaufvertrags unbedingt erforderlich sind. Erwirbst du eine App für dein Smartphone, musst du in der Regel das Betriebssystem (Google Android, Apple iOS, Windows Phone) und die Version des Betriebssystems preisgeben. Eine Börsen-App, die den Kurs der georderten Aktien anzeigt, muss zu ihrer Funktionsweise nicht das gesamte Telefonbuch, sämtliche E-Mail-Adressen und die Seriennummer des Handys (IMEI) an den App-Anbieter übertragen. Auch darf der Anbieter die Personendaten, die er zur Abwicklung des Lizenzvertrages erhalten hat, nicht an Werbe-Agenturen weitergeben. Ebenso dürfen die Personendaten beispielsweise für Newsletter zu „interessanten Neuheiten" nicht ungefragt verwendet werden.

Rechte der Betroffenen

Der Datenschutz schützt ein selbstbestimmtes digitales Leben. Dies setzt voraus, dass der Internetnutzer jederzeit die Datenverarbeitung kontrollieren kann, d. h. der Einzelne soll die Möglichkeit haben, die Verarbeitung seiner Daten zu beeinflussen und unter Umständen auch zu blockieren. So sieht der Datenschutzkodex Transparenz-, Steuerungs- und Sanktionsrechte vor.

Das wichtigste Betroffenenrecht ist das Auskunftsrecht. Betroffene haben das Recht, sich bei der verantwortlichen Stelle darüber zu informieren, welche Daten zu seiner Person gespeichert sind, woher die Daten stammen, für welchen Zweck sie verwendet werden und an wen sie weitergeleitet wurden.

Ist der Betroffene über die Datenverarbeitung informiert, kann er die Rechtmäßigkeit der Datenverarbeitung beurteilen und falls nötig, weitere Rechte geltend machen. Stellt sich heraus, dass die Internetfirma unrichtige Personendaten gespeichert hat, hat der Betroffene ein Recht darauf diese zu berichtigen. Hat die Internetfirma die Daten widerrechtlich gespeichert, kann er ihre Löschung verlangen.[111]

Bei Rechtsverstößen stehen dem Betroffenen Sanktionsrechte zu. Der Betroffene kann die Datenschutzbehörde Garante Privacy[112] anrufen, er kann Schadensersatz verlangen oder Strafantrag stellen, falls auch das Strafrecht verletzt wurde.

Die Betroffenenrechte sind durch die allgegenwärtige Datensammelei im Netz gefährdet. Haben die Anbieter von Webseiten, Suchmaschinen, eShops oder sozialen Netzwerken ihre Web-Server im außereuropäischen Ausland, dann ist das Datenschutzrecht schwer durchsetzbar. Der Verletzte muss zunächst stichhaltig darlegen, dass der Web-Anbieter dem italienischen Datenschutzrecht unterliegt und nachweisen, dass dieser tatsächlich das Datenschutzrecht verletzt hat. Weiters muss er die Identität des Verletzers ermitteln. Dies ist schwierig, sollten die Angaben im Impressum falsch sein. Der Betreiber des Webservers, auf dem die Webseite gehostet ist, ist nur auf der Grundlage eines Gerichtsbeschlusses verpflichtet, die tatsächliche Identität des Inhabers der Webseite preiszugeben.

Auskunftsrecht

>Vorname und Name<
>Straße/Hausnummer<
>Land/PLZ/Ort<
>E-Mail-Adresse<

>Firma<
>Straße/Hausnummer<
>Land/PLZ/Ort<

Auskunftsrecht über die eigenen Daten gemäß Art. 7 D.lgs. 196/2003

Der unterfertigte >Vorname Name<, wohnhaft in >Wohnort<, verlangt gemäß Art. 7 Absatz 2 D.lgs. 196/2003 Auskunft über:

- Über welche Daten zu meiner Person verfügen Sie?
- Woher haben Sie diese Daten erhalten?
- Für welchen Zweck haben Sie die Daten verarbeitet?
- An wen haben Sie die Daten weitergeleitet?

Zur Erfüllung meiner Forderung setze ich Ihnen eine Frist bis zum >Datum< (14 Tage später). Sollten Sie diese Forderung ignorieren, behalte ich mir weitere rechtliche Schritte vor.

Mit freundlichen Grüßen

>Ort, Datum<
>Unterschrift<

111 Der EuGH hat im Mai 2014 ein „Recht auf Vergessen“ beschlossen. Laut EuGH-Urteil können Suchmaschinen-Betreiber wie Google dazu verpflichtet werden, Links zu Webseiten mit sensiblen persönlichen Daten aus ihren Suchergebnissen zu löschen. Google muss bei jedem Löschantrag zwischen dem Recht auf ungehinderten Zugang zu Informationen und dem auf Privatheit miteinander abwägen. Kommt Google dem Löschantrag nicht nach, kann sich der Betroffene an die nationale Datenschutzbehörde oder das zuständige nationale Gericht wenden: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf; Google Web-Löschantrag: https://support.google.com/legal/contact/lr_eudpa?product=websearch#

112 www.garanteprivacy.it

2.2.2 Schutz durch Technik

> „In einer durch und durch technisierten Welt hat Selbstbestimmung nur dann eine Chance, wenn sie technisch unterstützt wird. Daher ist Datenschutzrecht auf Datenschutztechnik angewiesen."
>
> Alexander Roßnagel, Rechtswissenschaftler

Soll das „informationelle Selbstbestimmungsrecht" als Grundrecht tatsächlich gewährleistet sein, muss es durch Technik ergänzt werden. Der rechtliche Schutz allein genügt im globalen Netz nicht, dieser muss durch ein Mindestmaß an Selbstschutz erweitert werden. Zur Selbsthilfe muss der Nutzer befähigt werden, im Netz Sicherheitstools zu suchen und bei der täglichen Arbeit routinemäßig anzuwenden. In diesem Abschnitt wollen wir uns auf die Kontrolle der Datenspuren in Word-, PDF-, MP3- und Foto-Dateien begrenzen.

2.2.2.1 Metadaten in Word-Dateien

Word-Dokumente enthalten mehr Informationen, als auf dem Papierausdruck zu sehen sind. Soll ein Word-Dokument vom Lektor auf Tipp- und Orthographiefehler korrigiert werden, dann ist es sinnvoll, dass die Bearbeitungshistorie nachverfolgt werden kann, damit der Verfasser die Korrekturen ansehen und dazu seine Zustimmung erteilen kann. Willst du hingegen eine Word-Datei auf eine Webseite stellen oder die Word-Datei deinem Arbeitgeber per E-Mail-zusenden, dann sollte sichergestellt sein, dass die Word-Datei nur solche Informationen enthält, die du kennst und die du auch veröffentlichen willst. Sollte der Internetnutzer oder der Arbeitergeber nicht zu Informationen gelangen, die er besser nicht bekommen sollte, musst du die Einstellungen deines Word-Programms ändern und persönliche Informationen aus der Word-Datei löschen.

MS Word 2013

Sollen im Word-Dokument Überarbeitungen und persönliche Daten für die Empfänger des überarbeiteten Textes sichtbar sein? Das hängt vom Verwendungszweck des Word-Dokumentes ab.

Änderungsmodus einschalten: Schreiben Studenten eine Abschlussarbeit, ist es unumgänglich, dass jemand den Text korrekturliest. Arbeiten mehrere Autoren an einem Text, wollen die Co-Autoren wissen, wer was im Text geändert hat. Aktiviere hierfür die Funktion *Änderungen nachverfolgen.* Klicke zunächst mit der rechten Maustaste in die Statusleiste am unteren Bildrand und passe sie so an, dass der Schriftzug *Änderungen nachverfolgen* angezeigt wird. Die Funktion kannst du ein- oder ausschalten, indem du einfach auf den Schriftzug klickst.

Überprüfe, ob du tatsächlich sämtliche Änderungen im Text sehen kannst. Wechsle dazu über den Reiter *Überprüfen* in die Gruppe *Änderungen nachverfolgen* und wähle rechts im Menü *Markup: alle* aus. Daraufhin klickst du auf das Menü *Markup anzeigen* und setzt vor *Kommentare, Freihand, Einfügungen und Löschen* und *Format* ein Häkchen. Nun musst du nur noch festlegen, in welcher Ansicht die Änderungen sichtbar sein sollen. Unter Markup anzeigen/Sprechblasen kannst du wählen, ob die Überarbeitungen im Text (inline) oder in *Sprechblasen* am Rande des Textes angezeigt werden sollen.

Änderungen annehmen oder ablehnen? So, nun bekommst du vom Lektor das Word-Dokument wieder per Mail zurück und gehst die Änderungen durch. Über den Reiter *Überprüfen,* Gruppe *Änderungen nachverfolgen,* kannst du fallweise nur auf das *Annehmen*- oder *Ablehnen*-Icon drücken. Damit wird nur die aktuelle Änderung angenommen oder abgelehnt und Word springt zur nächsten Änderung. Bist du mit sämtlichen Korrekturen einverstanden, dann gehe unter *Änderungen nachverfolgen* zum Icon mit dem Bestätigungshaken *Annehmen,* klicke auf das kleine Dreieck darunter und wähle im geöffneten Menü *Alle Änderungen annehmen*. Sind die Änderungen unakzeptabel, machst du dasselbe über das Icon *Ablehnen*.

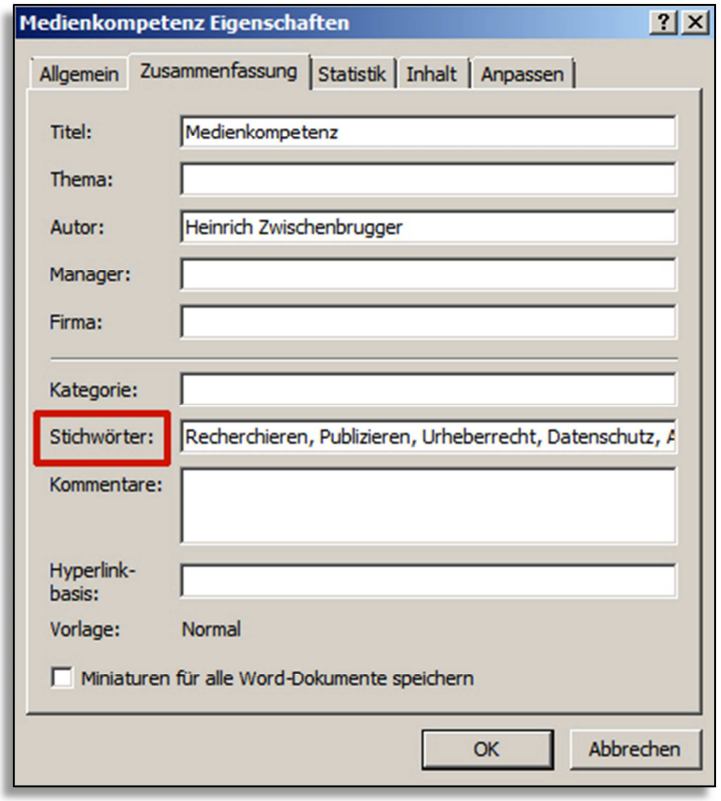


Abb. 14: Word-Dokument Eigenschaften

Datenspuren beseitigen: Wie muss man vorgehen, dass beispielsweise der Vertragspartner oder die Behörden nur das finale Word-Dokument erhalten? Schalte zunächst über die Statusleiste *Änderungen nachverfolgen* aus. Wechsle dann zu *Datei/Informationen* und klicke dort auf die Schaltfläche *Auf Probleme überprüfen*. Im geöffneten Menü wählst du *Dokument prüfen* und es erscheint eine Übersicht, in der du die Datenspuren des Word-Dokuments sehen kannst. Wichtig ist der Punkt *Kommentare, Überarbeitungen, Versionen und Anmerkungen*. Klicke auf *Prüfen* und dann auf die Schaltfläche *Alle entfernen* und die unerwünschten Überarbeitungsspuren werden gelöscht. Soll der Empfänger des Dokuments auch nicht wissen, wer den Text verfasst hat, musst du die Datei von persönlichen Informationen säubern. Dafür musst du hinter dem Punkt *Dokumenteigenschaften und persönliche Informationen* auf die Schaltfläche *Alle entfernen* drücken.

Einzelne Eigenschaften des Dokuments kannst du auch manuell ändern. Gehe dazu über *Datei/Informationen* rechts oben auf *Eigenschaften* und klicke im Auswahlmenü auf *Erweiterte Eigenschaften*. Unter dem Reiter *Allgemein* findest du allgemeine Informationen über das Dokument. Öffne den Reiter *Zusammenfassung* und gib

die Informationen ein, die in den einzelnen Eigenschaftsfeldern enthalten sein sollen. Die Stichwörter dienen der inhaltlichen Erschließung des Word-Dokuments und sollen deshalb überlegt gewählt werden.

LibreOffice 5.xx

Auch die Freeware LibreOffice[113] ermöglicht dir, die persönlichen Daten (Metadaten) aus dem Dokument zu entfernen sowie Bearbeitungen nachzuverfolgen. Zu den Infos zum Verfasser des Dokuments gelangst du über den Menüpunkt *Extras/Optionen*….Im Optionenfenster klickst du unter *LibreOffice* auf *Benutzerdaten*. Hier kannst du den Vor- und Zunamen und/oder an deren Stelle ein Kürzel eintragen. Sollen keine Details über den Autor an andere weitergegeben werden, kann du sie auch aus dem Dokument entfernen.

Wie aktiviert man den Änderungsmodus in LibreOffice? Zunächst musst du das zu bearbeitende Dokument öffnen. Darauf gehst du unter dem Menüpunkt *Bearbeiten* zu *Änderungen verfolgen* und drückst dann im Auswahlmenü auf *Änderungen aufzeichnen*. Nun nimmst du die gewünschten Änderungen im Text vor. Alle neu eingefügten Textpassagen werden farbig unterstrichen und die gelöschten farbig durchgestrichen. Zu jeder Änderung kannst du auch einen Kommentar hinzufügen. Setze hierzu den Textcursor in den Bereich der Textänderung, klicke dann unter dem Menüpunkt *Bearbeiten* auf *Änderungen verfolgen* und weiter auf *Änderungen kommentieren…* Willst du die Aufzeichnung der Änderungen beenden, dann gehe erneut unter dem Menüpunkt *Bearbeiten* zu *Änderungen verfolgen* und wähle die Markierung bei *Änderungen aufzeichnen* ab.

Erhältst du ein überarbeitetes Dokument beispielsweise von deinem Lektor, kannst du die vorgenommenen Änderungen billigen oder auch verwerfen. Gehe dazu im Menü *Bearbeiten* über *Änderungen verfolgen* zu *Änderungen verwalten*…. Daraufhin öffnet sich das Dialogfenster *Änderungen verwalten* mit einer Liste der vorgenommenen Änderungen. Du kannst nun jede Änderung einzeln oder auch alle in einem Rutsch akzeptieren oder ablehnen.

Du kannst auch noch die Eigenschaften des geöffneten Dokuments bearbeiten. Dazu klickst du auf den Menüpunkt *Datei* und dann auf *Eigenschaften….* Öffne nun den Reiter *Allgemein*. Sollen keine Benutzerdaten aufscheinen, dann musst du das Häkchen vor *Benutzerdaten verwenden* entfernen. Soll auch nicht ersichtlich sein, wann das Dokument ursprünglich erstellt und später geändert wurde, drückst du auf den Button *Zurücksetzen*. Wechsle nun zum Reiter *Beschreibung*. Im folgenden Dialogfenster kannst du die Eigenschaften des Dokuments bearbeiten oder auch gänzlich entfernen. Mit einem Klick auf *OK* ist die Bearbeitung der Metadaten abgeschlossen.

113 http://de.libreoffice.org; https://www.libreoffice.org/download

2.2.2.2 Metadaten in PDF-Dateien

Word-Dokumente kannst du auch ins PDF-Format konvertieren. Bei einer PDF-Datei hast du die Sicherheit, dass sie im Nachhinein von anderen nicht geändert werden kann. Zudem ist das PDF-Format ein plattformunabhängiges weitverbreitetes Dateiformat. Mithilfe des Freeware-Tools PDFCreator[114] können Dokumente vom Word-Format einfach in das PDF-Format konvertiert werden. Bei der Umwandlung erscheint ein Dialogfenster, in welchem du die Eigenschaften des PDF-Dokuments festlegen kannst.

PDF-Writer setzen mitunter Metadaten wie Titel, Autor oder Bearbeitungszeit automatisch. Doch nicht in jedem Fall sollen solche Metadaten für Leser sichtbar sein. Mit der Freeware BeCyPDFMetaEdit[115] lassen sich diese in PDF-Dokumenten beliebig editieren. Starte das Tool und lade die zu editierende PDF-Datei. Die Dateien können in drei Modi geöffnet werden: Im *Inkrementellen Update*-Modus werden die ursprünglichen Dateien nicht gelöscht, sondern nur überschrieben – die ursprünglichen Metadaten könnten später wieder hergestellt werden; im *Vollständigen Neuschreiben*-Modus dagegen gehen alle ursprünglichen Metadaten verloren; im *Reparieren*-Modus schließlich lassen sich u. U. defekte PDF-Dateien wiederherstellen. Sollen die Metadaten (XMP) entfernt werden, musst du den Reiter *Metadaten (XMP)* öffnen und *XMP-Metadaten beim Speichern des Dokuments entfernen* aktivieren. Sind die Änderungen abgeschlossen, klickst du auf die Schaltfläche *Speichern unter…*.

Stichworte und Nutzungsarten festlegen

Die Stichworte einer PDF-Datei sollen den Inhalt des Dokuments richtig beschreiben, damit dieser im Netz leichter auffindbar ist. Regeln für die richtige Beschreibung von Internetdokumenten stellt z. B. der Dublin Core bereit.[116] Manchmal kann es sinnvoll sein, auch die Nutzungsrechte in PDF-Dokumenten festzulegen, etwa wenn sichergestellt werden soll, dass der Leser den Inhalt des Dokuments nicht ändern kann. Stichworte und Nutzungsarten kannst du bequem mit dem Programm PDFCreator festlegen.

Wähle als Drucker für dein Word-Dokument den PDFCreator aus. Als erstes gibst du im Bereich Metadaten die passenden Stichworte ein. Darauf drückst du auf den Button *Einstellungen* und gehst im Dialogfenster *Profileinstellungen* über *PDF* zum Reiter *Sicherheit*. Hier kannst du im Einzelnen festlegen, was der Nutzer mit dem PDF-Dokument tun darf und was nicht. (vgl. Abb. 15).

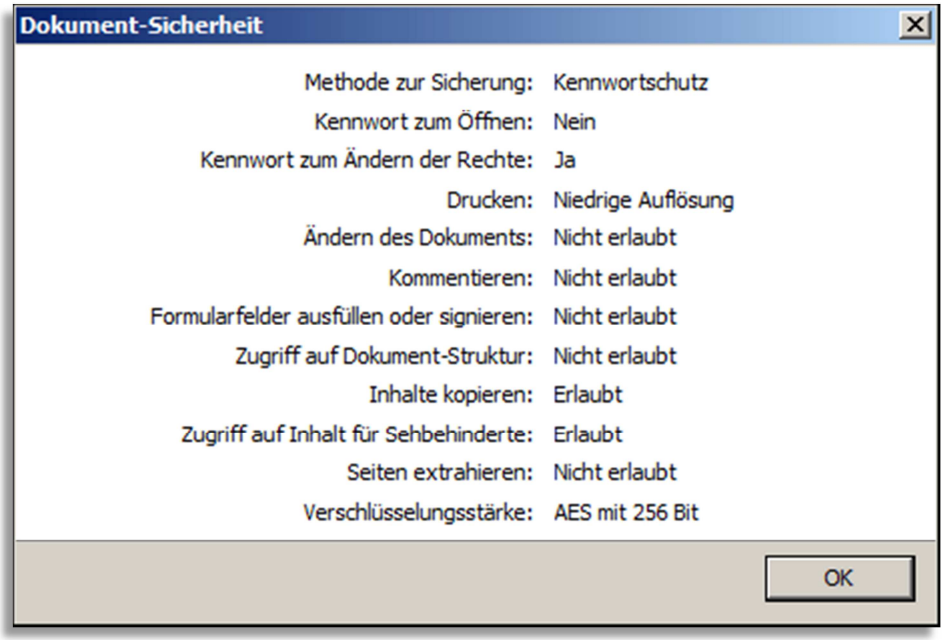
---

114 http://de.pdfforge.org/pdfcreator
115 www.becyhome.de
116 http://dublincore.org/; „Dublin Core“. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 5. Mai 2015, 12:39 UTC. URL: http://de.wikipedia.org/w/index.php?title=Dublin_Core&oldid=141793180 (Abgerufen: 11. Juni 2015, 16:54 UTC)

2.2.2.3 Metadaten in Audio-Dateien

Musikdateien enthalten sogenannte ID3-Tags. Mit der Freeware Mp3tag,[117] TagScanner[118] oder Audacity[119] kannst du manuell die ID3-Tags von MP3-Audio-Dateien entfernen, hinzufügen oder ändern. Du kannst die richtigen Tags auch von sogenannten CDDB-Datenbanken (Compact Disc Database) aus dem Internet abfragen und automatisch in deine Musikbibliothek importieren.

So geht's mit dem Audio-Editor Audacity: Starte das Programm, öffne die Audiodatei, deren Metadaten du bearbeiten willst, klicke auf *Datei* und darauf auf *Metadaten-Editor…*. Im geöffneten Metadaten-Fenster kannst du die einzelnen Eigenschaften der Audio-Datei bearbeiten.


Dokument-Sicherheit
Methode zur Sicherung: Kennwortschutz
Kennwort zum Öffnen: Nein
Kennwort zum Ändern der Rechte: Ja
Drucken: Niedrige Auflösung
Ändern des Dokuments: Nicht erlaubt
Kommentieren: Nicht erlaubt
Formularfelder ausfüllen oder signieren: Nicht erlaubt
Zugriff auf Dokument-Struktur: Nicht erlaubt
Inhalte kopieren: Erlaubt
Zugriff auf Inhalt für Sehbehinderte: Erlaubt
Seiten extrahieren: Nicht erlaubt
Verschlüsselungsstärke: AES mit 256 Bit
OK
Abb. 15: Dokument-Sicherheit

2.2.2.4 Metadaten in Foto-Dateien

Was sind Exif-Daten?

Digitale Kameras speichern neben dem eigentlichen Bild auch die sogenannten Exif-Daten ab. Exif-Daten zeigen die Aufnahmeinformationen der Kamera an, wie Datum und Uhrzeit, Belichtungszeit, Brennweite, Blende, ISO-Wert sowie Kamerahersteller und Kameramodell. Einige Kameramodelle halten auch den genauen Aufnahmestandort in den Exif-Daten fest.

Was kann man mit den Exif-Daten anfangen? Das hängt vom Verwendungszweck ab. Kennen Fotografen die Aufnahmedaten eines Fotos, können sie diese später am PC analysieren und versuchen aus den aufnahmetechnischen Fehlern zu lernen. Will der Fotograf das Motiv hervorheben und störende Details im Hintergrund unscharf werden lassen, muss er eine offenere Blende wählen. Eine zu lange Belichtungszeit macht deutlich, warum das Foto verwackelt ist. Wer mehrere Kameras verwendet, kann die Fotos einer bestimmten Kamera zuordnen. Wird auch der Aufnahmeort in der Bilddatei abgespeichert, gibt es kein Rätselraten mehr, wo ein

117 http://www.mp3tag.de/
118 http://www.xdlab.ru/en/index.htm
119 http://audacity.sourceforge.net

Foto geknipst wurde. Bei langen Reisen lässt sich später aus den Ortsdaten die Reiseroute exakt ermitteln.

Exif-Daten bearbeiten oder löschen

Die Exif-Daten lassen sich im Nachhinein auch bearbeiten und löschen. Eine Bearbeitung kann sinnvoll sein, wenn an der Kamera die Winterzeit statt der Sommerzeit eingestellt war und die Zeitverschiebung korrigiert werden soll; oder wenn später Standortdaten manuell hinzugefügt werden sollen. Ist im Smartphone das Speichern von GPS-Daten standardmäßig aktiviert, verrät ein Foto aus der eigenen Wohnung mit dem Upload in ein soziales Netzwerk ungewollt den Wohnort des Nutzers. Von Dieben können solche Standortdaten praktischerweise für den nächsten Wohnungseinbruch missbraucht werden. In einem solchen Fall kann es wichtig sein, die Exif-Daten eines Fotos zu löschen, bevor es ins Netz gestellt wird. Die meisten Bildbearbeitungsprogramme können die Metadaten auslesen. Mit dem Tool pyExifToolGUI,[120] das eine grafische Oberfläche (GUI) für das Kommandozeilenprogramm ExitTool ist, kannst du nicht nur die Metadaten auslesen, sondern auch teilweise bearbeiten und löschen.

Wie geht’s? Öffne das Programm und lade zunächst über die Schaltfläche *Load Images* unten links die Fotos, deren Metadaten du bearbeiten willst. Markiere die Fotos in der Fotoliste und öffne über das Kontextmenü die passende Funktion. Das Kontextmenü bietet beispielsweise die Optionen, das Datum neu festzulegen oder die Metadaten zu entfernen. Unter *Edit Data/Gps* können die Standortdaten manuell eingetragen werden. Kennst du die Ortsdaten noch nicht, kannst du diese über den Button *OpenMapCoordinates.net* ermitteln und per Copy & Paste ins Programm importieren.

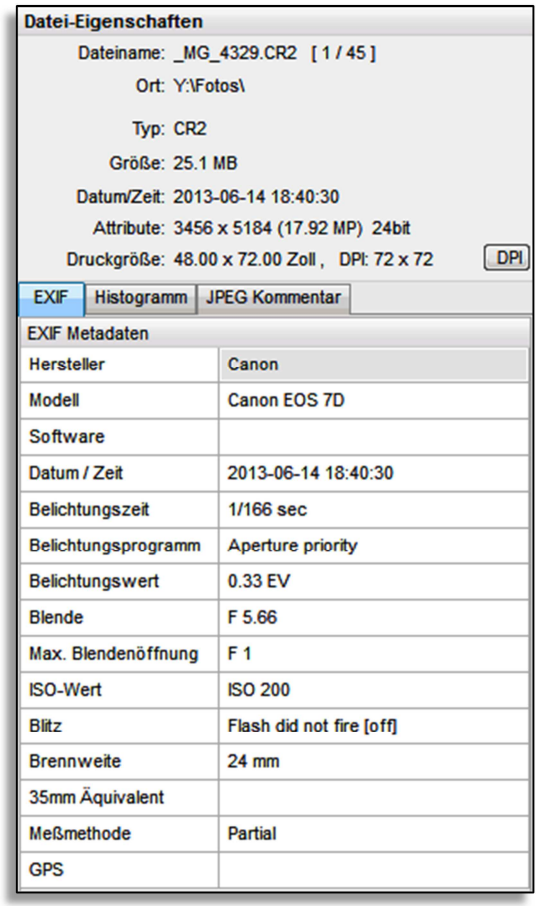


Abb. 16: Bildeigenschaften

Fotos verschlagworten

Wer gerne fotografiert, hat schnell ein paar Tausend Fotos auf dem Datenträger. Zudem stellen immer mehr Nutzer ihre Fotos in soziale Netzwerke und Fotoportale. Mit dem rasanten Anstieg der Fotomenge wird es für Nutzer immer schwieriger, Fotos mit bestimmten Motiven zu finden. Werden Fotos mit einem oder mehreren Tags versehen, sind sie später schneller auffindbar. Tags sind Schlagwörter, die den Bildinhalt angemessen beschreiben. Haben Hobbyfotografen 10.000 Fotos auf dem Datenträger, können sie

120 Webseite des Entwicklers: https://hvdwolf.github.io/pyExifToolGUI/

mithilfe von Schlagwörtern die Suche nach einem bestimmten Foto auf wenige Fotos eingrenzen. Programme für die Fotoverwaltung ermöglichen in der Regel Fotos zu verschlagworten.

Software	Webadresse	Fotos verschlagworten (taggen)
Gimp	http://www.gimp.org	Öffne das Foto, klicke auf *Datei/Eigenschaften*. Gehe im Dialogfeld *Eigenschaften* auf die Registerkarte *Beschreibung*. Hier kannst du die Stichwörter zum Bild eingeben.
Picasa	http://picasa.google.com	Starte das Programm, öffne das Foto und gehe zu *Ansicht/Tags*. Im Tag-Fenster, am rechten Bildrand, kannst du die Metadaten eingeben.
Zoner PhotoStudio Free	http://free.zoner.com/de	Lade das Foto. Klicke im Menüpunkt *Viewer* auf *Datei/Bildinformation*, anschließend unter dem Vorschaubild auf das *Drop-Down-Menü* und dann auf *Schlüsselwörter*. Über die Google Maps-Karte können auch Standortdaten zur Aufnahme hinzugefügt werden.

Tab. 10: Software für Foto-Tags und Fotoverwaltung

Mit welchen Schlagworten sollte man Fotos versehen? Sinnvoll sind Schlagwörter zu den Fragen: Wo? Wann? Wer? Was? Auf die Frage, wo wurde das Foto aufgenommen, kannst du das Land, die Region und den Ort angeben, z. B. Spanien, Granada. Wann wurde das Foto aufgenommen? Zeitangabe: Jahr, Monat, Tag, Uhrzeit. Wer ist auf dem Foto sehen? Bei bekannten Personen Vor- und Zuname; bei unbekannten Personen ihre Charakteristika, etwa „Frau“, „Regenschirm“. Was ist auf dem Foto zu sehen? Versuche, das Hauptmotiv des Fotos zu beschreiben. Bei einem Ausflug nach Granada in Spanien fotografierst du etwa die Stadtburg Alhambra: „Urlaub“, „Spanien“, „Granada“, „Alhambra“, „Architektur“, „Datum“, „Uhrzeit“. Es gibt zahlreiche kostenlose Programme, mit denen du deine Bilder verschlagworten kannst.

2.3 Eigene oder fremde Webseite?

Wer im Netz Inhalte veröffentlichen will, steht vor der Entscheidung, die Inhalte auf einer eigenen oder unter einer fremden Webseite zu veröffentlichen. In vielen Fällen stellt sich die Frage nicht, weil ein Status-Update auf Facebook, ein Angebot bei eBay, eine Korrektur eines Beitrags auf Wikipedia oder eine Produktbewertung bei einem Online-Shop nur auf einer fremden Webseite erfolgen kann. Blogger hingegen müssen abwägen, ob sie ihre Inhalte auf einer eigenen oder auf einer fremden Webseite publizieren.

2.3.1 Eigene Webseite

Eine eigene Webseite bietet mehr Freiheiten, weil man „Herr im Hause“ ist. Wer auf fremden Webseiten Inhalte veröffentlicht, muss deren „Hausordnung“ akzeptieren, damit rechnen, dass die Nutzungsbedingungen jederzeit abgeändert sowie die Webseiten geschlossen werden können.

Wird die eigene Webseite geschäftsmäßig genutzt, also werden Inhalte, Waren oder Dienste gegen Entgelt angeboten, ist ein Impressum Pflicht. Die Funktion des Impressums ist, dass der Nutzer bzw. der Kunde weiß, wer der Anbieter ist, er kann recherchieren, ob dieser vertrauenswürdig ist und an wen er sich im Falle von Rechtskonflikten wenden kann. Zu den Pflichtangaben im Impressum gehören u. a. der Name und die Anschrift des Anbieters, der Sitz der Firma, Kontaktadressen, Vertretungsberechtigte, Handelsregister- und Steuernummer. Die Angaben des Impressums müssen für den Nutzer „leicht erkennbar und unmittelbar erreichbar“ sein. Das ist dann der Fall, wenn das Impressum bereits auf der Startseite zu sehen ist. Anstelle von Impressum kann auch die Bezeichnung „Anbieterkennzeichnung“, „Kontakt“ oder „Über uns“ stehen. Fehlt das Impressum, riskieren Seitenbetreiber und Firmen eine Abmahnung.

2.3.2 Fremde Webseite

Die Gründe auf fremden Webseiten zu publizieren, können höchst unterschiedlich sein. Firmen wollen beispielsweise neben ihrer eigenen Homepage auf sozialen Netzwerken, wie Facebook & Co. einen zusätzlichen Marketingkanal eröffnen und mit Kunden in eine Interaktion treten. Autoren des Wikipedia-Projektes arbeiten unentgeltlich an der freien Enzyklopädie Wikipedia, legen Artikel an und bearbeiten vorhandene Artikel. Junge Autoren verdienen mit Büchern zunächst kein Geld, erst mit dem „Drumherum“ entstehen Einnahmen. Denn Autoren schreiben nebenbei Blogeinträge, twittern, beliefern die Chroniken anderer bei Facebook

„mit Einfällen, Aphorismen und Kommentaren und laden kleine Videobeiträge von sich aus bei YouTube hoch, die sie dann wiederum auf anderen Plattformen und im eigenen Blog verlinken.“[121] Bürgerjournalisten veröffentlichen ihre Beiträge in einem Communityportal, weil sie dort mehr Leser, Reaktionen und Diskussionen erwarten.

Kunden bewerten Produkte bei Online-Shops und geben Rezensionen zu Büchern oder DVDs ab. Damit helfen sie anderen Kunden, eine informierte Einkaufsentscheidung zu treffen. Positive Bewertungen bewirken Wettbewerbsvorteile für Anbieter, egal ob für Reiseveranstalter, Finanzberater oder Friseure. Bewerter werden so zu Werbeträgern für Produkte und Anbieter. Nutzer können auf Facebook & Co kostenlos Privates und Geschäftliches tauschen. Im Gegenzug vermarkten die Betreiber der sozialen Plattformen die Nutzerdaten an die Werbeindustrie.

Wer auf fremden Webseiten publiziert, unterliegt deren Nutzungs- und Datenschutzbedingungen. So können Nutzungsbedingungen von Online-Zeitungen etwa vorsehen, dass nur sachliche Leserkommentare veröffentlicht werden, dass ein „Grilloscone“-Stil[122] unerwünscht ist und dass Leserkommentare, die „Hassbotschaften, Volksverhetzung, Diskriminierung und Gewaltverherrlichung“ beinhalten, nicht veröffentlicht werden. Für Nutzer kann es wichtig sein, zu wissen, für welche Zwecke die eigenen Daten verwendet werden und ob sie zureichend vor Angriffen der Cyberkriminellen geschützt sind. Schließlich müssen Nutzer fremder Webseiten damit rechnen, dass die Webseite vom Netz genommen werden kann, wenn Investoren nicht mehr vom Geschäftsmodell des Web-Angebots überzeugt sind.

Die Impressumspflicht besteht auch auf fremden Webseiten, wenn sie geschäftsmäßig genutzt werden, etwa wenn eine Firma eine „Page“ für Marketingzwecke auf Facebook betreibt oder wenn bezahlte Werbebanner auf der Webseite eingeblendet werden.

121 http://www.zeit.de/kultur/literatur/2011-09/netzliteratur-essay

122 Beppe Grillo ist ein professioneller Komiker und machte in Italien bei den Parlamentswahlen Februar 2013 durch seine populistische Wahlkampagne von sich reden.

2.4 Arbeitsaufträge

1. Das Thema kreist um die Funktionsweise des Wiki-Prinzips. Bildet in der Klasse Zweiergruppen und teilt jeder Gruppe einen Buchstaben zu.

   Erster Schritt: Jede Gruppe erstellt eine Werbe-Webseite zum Thema Bioland Obervinschgau (auch eine andere Region). Zu Beginn klärt jede Gruppe u. a. Domain, Logo, Texte, Schriftgröße, Schriftfarbe, Fotos und Links der Webseite. Ist sich die Gruppe über das Konzept einig, entwirft sie hierzu ein Plakat.

   Zweiter Schritt: Jede Gruppe bewertet und verbessert die Werbe-Webseite der Gruppe mit dem nachfolgenden Buchstaben und protokolliert die Gründe für die durchgeführten Änderungen, also warum sie etwa die Position eines Fotos verändert oder es entfernt hat.

   Dritter Schritt: Wählt nun per Mehrheitsentscheidung die beste Werbe-Webseite aus.

   Vierter Schritt: Diskutiert Regeln, wie vorgegangen werden sollte, dass am Ende die qualitativ beste Werbe-Webseite gewählt wird.

2. Was musst du tun, damit Texte oder Fotos, die du auf soziale Netzwerke oder auf deine Webseite hochlädst und veröffentlichst, urheberrechtlich geschützt sind?

3. Recherchiere, welche Nutzungsrechte du dem sozialen Netzwerk Facebook oder dem Fotoportal Flickr beim Upload deiner Fotos einräumst?

4. Darfst du alles aus dem Internet zitieren, sofern du die Quelle angibst?

5. Darfst du ohne Erlaubnis des Rechteinhabers von einer fremden Webseite ein Foto kopieren und auf dein Facebook-Profil einstellen.

6. Darf die Schule so ohne Weiteres Fotos von Schulklassen machen und diese auf der Schulwebseite veröffentlichen? Gilt das Recht am eigenen Bild auch für Schüler?

7. DJ Kevin weiß, dass er nicht einfach fremde Musik spielen darf. Darf er aber ohne Lizenz sampeln, also kurze Ausschnitte aus fremder Musik verwenden?

8. Recherchiere zumindest nach zwei Musikportalen, die Musik unter die Sampling-Lizenz von Creative Commons stellen und was diese besondere Lizenz erlaubt.

9. Du willst die Fassade einer sanierten Jugendstilvilla fotografieren, aber davor steht ein Tourist. Musst du den Touristen um Erlaubnis fragen, bevor er mit aufs Bild kommt?

10. Darfst du eine Wasserburg von einer öffentlichen Straße aus fotografieren und auf deinen Weblog oder auf eines der sozialen Netzwerke hochladen?

11. Überprüfe, ob die Käufer eines Windows- oder eines Apple iOS-Betriebssystems ein einfaches oder ein ausschließliches Nutzungsrecht daran erwerben.

12. Überlegt zu zweit, welche Lizenznehmer ein Interesse an ausschließlichen Nutzungsrechten an Fotos haben. Stellt eure Thesen der Klasse vor.

13. Diskutiert zu zweit, wie im Internet Fanseiten über Film- oder Popstars urheberrechtlich zu bewerten sind. Dürfen Fans Fotos von ihren Idolen, Videoclips aus Kinofilmen oder Screenshots von der neuen CD so ohne Weiteres auf ihre Fanseite hochladen? Fallen die Inhalte von Fanseiten, wie Fotos, Texte, Videos oder Audios unter das Zitatrecht? Unter welchen Voraussetzungen dürfen Fans aus fremden Werken zitieren? Wie ist die Rechtslage?

14. Erlaubt das Urheberrecht CD-Covers aus Internet-Datenbanken herunterzuladen und zu privaten Zwecken als Labels direkt auf die gebrannten Blu-rays, DVDs und CDs zu drucken?

15. Deine Schulklasse will zum Thema Betriebspraktikum einen Film drehen. Welche urheberrechtlichen und leistungsschutzrechtlichen Fragen stellen sich hierbei? Erstellt zu zweit eine Rechte-Checkliste für die Filmproduktion.

16. Angenommen, die Studenten der Universität Bozen programmieren eine Software speziell für Kleinunternehmer zur Abwicklung des Zahlungsverkehrs mit Online-Banken. Das Projekt wird vom Handwerkerverband und von der Landesregierung unterstützt.
    a) Welche (urheberrechtlichen) Rechtsfragen sollten geklärt sein, bevor die Software veröffentlicht wird?
    b) Verfasst zu viert eine Checkliste zur Softwarelizenz.
    c) Unter welcher Lizenz sollte die Software angeboten werden – als Freeware, als Open-Source-Lizenz oder als proprietäre Lizenz („End User Licence Agreement“, EULA)?
    d) Wann sollte der Nutzer vom Inhalt des Lizenzvertrages in Kenntnis gesetzt werden: vor dem Erwerb, vor der Installation oder erst vor der ersten Inbetriebnahme des Programms (vgl. Art. 1341 c.c.)?

17. Welche Medienanbieter haben ein Interesse auf technischen Kopierschutz? Recherchiert, welche Kopierschutztechniken es zurzeit für die einzelnen Medien wie Texte, Fotos, Videos oder Audios gibt.

18. Darf man aus einem Musikstück mit einem Audio-Editier-Programm, wie Audacity[123] einen Teil herausschneiden, in das passende Format konvertieren, auf das Handy übertragen und als Klingelton nutzen?

19. Recherchiert zu zweit nach Handyklingeltönen, die unter der CC-Lizenz angeboten werden. Überprüft auch, was die CC-Lizenz konkret erlaubt und was nicht.

20. Macht das Urheberrecht einen Unterschied zwischen künstlerisch hochwertigen Fotos und Knipsbildern?

21. Darfst du eine Original-CD, die urheberrechtlich geschützt ist, rippen und über eine Tauschbörse zum Download anbieten?

22. Ist es erlaubt, Medieninhalte, die unter der CC-Lizenz stehen, über eine Tauschbörse oder einem Share- oder One-Click-Hoster zum Download anzubieten?

23. Recherchiere, wie die Medienindustrie die Identität des Anbieters ermittelt, der rechtswidrig geschützte Inhalte, wie Audios, Videos oder Computerspiele über Tauschbörsen oder Filehoster anbietet. Stelle die rechtlichen und sachlichen Zusammenhänge grafisch dar und informiere die Klasse darüber.

24. Wo kann man sich darüber informieren, unter welcher Lizenz Software (proprietäre Lizenz, Freeware, Open-Source, Freie Software) angeboten wird?

25. Für den Verkaufserfolg bei eBay zählt neben der richtigen Produktbeschreibung auch ein ansprechendes Produktfoto, denn es gilt „Ein Bild sagt mehr als tausend Worte“. Darf der Versteigerer Produktfotos von der Webseite des Herstellers verwenden?

26. Du erhältst den Auftrag, eine Homepage für einen Zimmervermieter zu erstellen. In die Homepage sollte auch eine Anfahrtsskizze eingebunden sein. Kläre die rechtliche Frage, ob du dazu einen Stadtplan aus einem Straßenatlas verwenden darfst.

27. Darfst du von einer kopiergeschützten Audio-CD eine Privatkopie brennen?

28. Von Software darf keine Privatkopie erstellt werden. Zulässig ist lediglich die Erstellung einer einzigen Sicherungskopie. Welche Lizenz erlaubt es, nach Belieben Privatkopien von Software zu erstellen und zu verbreiten?

123 http://audacity.sourceforge.net/

29. Die Schüler sollen sich mit dem Modell der CC-Lizenz befassen. Dazu sollen sie die einzelnen Symbole und die möglichen Kombinationen der CC-Lizenz auf ein Plakat malen. Außerdem sollen sie Thesen formulieren, wer ein Interesse an den einzelnen Symbolen und den möglichen Kombinationen hat.

30. Darfst du auf deinem Blog einen Link zu einem Videoclip von YouTube setzen?

31. Darfst du eine legal erworbene Musik-CD auf den PC rippen und die Audiodatei daraufhin auf dein Smartphone überspielen?

32. Erstellt zu zweit eine Checkliste zur Frage, was urheberrechtlich beim Drehen eines Videos zu beachten ist, das später auf YouTube hochgeladen werden soll.

33. Die Problematik des Urheberrechts kann über das Stationenlernen bearbeitet werden. Bildet drei Gruppen.

    Gruppe A beschäftigt sich mit den Fragen der Privatkopie und der Veröffentlichung von Musik. Die Gruppe erhält ein Stationenschild mit Thema, Namen der Schüler und einen Fragenkatalog. Die Schüler sollen den Fragenkatalog (zumindest) mit drei Fragen erweitern. Die Antworten schreiben die Schüler auf die Rückseite der Karten.

    a) Was versteht man unter einer Privatkopie?
    b) Darf man von einer Original Musik-CD eine Privatkopie erstellen?
    c) Darf man eine Privatkopie von einer kopiergeschützten Musik-CD erstellen?
    d) Darf man einen Fernsehfilm per TV-Karte aufnehmen, die Filmmusik extrahieren und auf den MP3-Player kopieren?
    e) Verletzt man das Urheberrecht, wenn man Musik aus dem eigenen MP3-Archiv auf der privaten Hauspartie abspielt?
    f) …

    Die Gruppe B beschäftigt sich mit Rechtsfragen zum Textwerk.

    Die Gruppe C untersucht Rechtsfragen zum Foto.

34. Bearbeitet und diskutiert das Modell der Kulturflatrate als eine Alternative zum klassischen Urheberrecht. Bildet hierfür drei Gruppen.

    Gruppe A beschäftigt sich mit dem Konzept der Kulturflatrate. Sie erhält ein Stationenschild mit Thema, Namen der Schüler und einen Fragenkatalog. Den Fragenkatalog erweitern die Schüler um weitere drei Fragen. Wie die Schüler die Antworten präsentierten, bleibt ihnen überlassen.

    a) Wie funktioniert das Modell Kulturflatrate?
    b) Wie werden die finanziellen Mittel auf Urheber und Verwerter verteilt?

c) Welchen Interessen dient die Kulturflatrate: den Urhebern, den Verwertern, den Nutzern?

e) …

Gruppe B beschäftigt sich mit den Schwächen der Kulturflatrate.

a) Wie wird die Qualität der Werke bei der Kulturflatrate berücksichtigt?

b) Wie wird der Erfolg der Werke gemessen und wer soll über die Verteilung der Mittel entscheiden?

Gruppe C recherchiert, welche Geschäftsmodelle zurzeit zur Finanzierung des Online-Journalismus erprobt und diskutiert werden und erstellt hierzu Kurzthesen.

35. Wie muss das Urheberrecht reformiert werden, damit das digitale Umfeld Anreize für Kreative zu weiteren schöpferischen Leistungen bietet?

36. Was kann passieren, wenn man Urheberrecht verletzt? Welche Folgen kann eine anwaltliche Abmahnung haben?

37. Ist der Betreiber eines privaten Blogs nach dem italienischen Datenschutzkodex verpflichtet, eine Datenschutzerklärung abzugeben?

38. Darf der Betreiber eines privaten Blogs aus Datenschutzgründen ein Webanalyse-Tool wie Piwik[124] nutzen? Wie lassen sich die Besucher eines Blogs identifizieren?

39. Gilt der Datenschutz auch für private Überwachungskameras? Darf man Kameras anbringen, um damit das eigene Haus und einen Teil des öffentlichen Bürgersteiges zu überwachen?[125]

40. Recherchiert, welche Flugpassagierdaten auf Flügen von Europa in die USA an die US-Behörden weitergeleitet werden und was mit diesen Daten passiert.

41. Das SWIFT-Bankdatenabkommen zwischen der EU und den USA ist seit dem 1. August 2010 in Kraft. Recherchiert, welche Regelungen das Abkommen beinhaltet und wer davon betroffen ist.

42. Welche Daten zählt der italienische Datenschutzkodex zu den personenbezogen Daten?

43. Unter welchen Voraussetzungen darf ein Online-Händler personenbezogene Daten an Werbeagenturen weiterleiten?

---

124 https://piwik.org/. Piwik untersucht die Herkunft der Blog-Besucher, welche Beiträge die Besucher aufrufen und wie lange diese angesehen werden und protokolliert die IP-Adresse der Besucher.

125 EUGH-Pressemitteilung (Rechtssache C-2012/13): http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-12/cp140175de.pdf

44. Recherchiert, wie Nutzer verhindern können, dass ihr Surfverhalten im Netz von Tools wie Google Analytics beobachtet und protokolliert wird.

45. Web-Händler dürfen nur dann Personendaten erheben, wenn der Betroffen dazu einwilligt und der Einwilligung eine Datenschutzbelehrung vorausgeht.

    a) Welche Angaben muss die Datenschutzbelehrung nach dem Datenschutzkodex enthalten?
    b) Wählt zwei lokale Online-Zeitungen aus und überprüft, welche Angaben die Datenschutzbelehrungen enthalten.

46. Der Internetkonzern Google macht mit dem Onlinedienst Google Street View Stadtrundfahrten im Internet möglich. Hierfür fährt im Auftrag von Google ein Auto mit einer 360-Grad-Kamera durch die Städte und macht detaillierte Fotos von Straßen und Häuserfronten. Darauf werden die Aufnahmen mit Standortinfos versehen und zu einem 3-D-Straßenatlas zusammengestellt. Verletzt Google mit diesem Dienst das „informationelle Selbstbestimmungsrecht“ der Bürger? Stellt Pro und Contra gegenüber.

3 Facebook klug nutzen

Leitfragen

- Wie funktioniert das Geschäftsmodell von Facebook?
- Welche persönlichen Informationen sollten nicht im Profil stehen?
- Was besagen das Opt-out- und das Opt-in-Prinzip?
- Wie kannst du festlegen, wer was von dir auf Facebook sehen oder lesen darf?
- Welche Rechtsvorschriften sind beim Posten von Texten oder Fotos zu beachten?
- Welche Mängel weist Facebook beim Thema Datenschutz auf?
- Wie kannst du dich gegen Cybermobbing zur Wehr setzen?
- Welche Alternativen gibt es zu Facebook?

3.1 Was ist Facebook?

Soziale Medien wie Facebook sind insbesondere für Jugendliche Teil ihres Alltagslebens. Sie nutzen soziale Netzwerke zu Albernheiten und zur Unterhaltung, bei der Pflege ihrer Beziehungen, zur Informationsbeschaffung sowie zum Lernen in der Schule. Per Handykamera teilen sie Aufgaben mit Mitschülern oder dokumentieren Tafelbilder für abwesende Schüler. Schüler können sich so Hausaufgabenhilfe leisten. Klassen können sich Gruppen zusammenschließen und gemeinsam ein Thema oder Dokumente bearbeiten. Kooperatives Arbeiten und Lernen ermöglicht Gespräche, die jede Schülerin und jeder Schüler der Klasse nur verfolgen oder sich auch daran beteiligen kann. Erschienen früher Fotos und Berichte zum Lehrausflug nach Wochen oder gar erst nach Monaten in der Schulzeitung, stehen heute bereits vor der Zugabfahrt die ersten Fotos und Kommentare auf Facebook - ohne Korrektur durch den Deutschlehrer und ohne Billigung durch die Zeitungsredaktion.

Facebook ist Teil der interaktiven Web 2.0-Angebote. Die Nutzer erstellen selbst Inhalte, Texte, Fotos oder Videos. Es handelt sich um eine neue Form der Selbstdarstellung sowie um soziale Interaktion und Gemeinschaft. Das birgt für den Nutzer Chancen, aber auch Risiken.

Alle können die Plattform unentgeltlich nutzen. Der Preis dafür ist freilich, dass Facebook die „Seele der Nutzer“ kennt. Facebooker, die etwas teilen oder mit einem „Gefällt mir“ versehen und Freundschaften knüpfen, versorgen Facebook mit ihren Interessen und Vorlieben. Die Daten nutzt Facebook für persönliche Werbung. Die Werbeeinnahmen verwendet die Firma für den Betrieb der Plattform und dazu, die Investoren bei Laune zu halten.[126]

Wie kann ein reflektierter und verantwortungsvoller Umgang mit Facebook aussehen? Voraussetzung dafür ist Medienkompetenz. Diese erfordert neben Bedienkompetenz, also zu wissen wie etwas geht, auch Urteilskompetenz. Zur Urteilsfähigkeit gehört, zu verstehen wie das Web 2.0-Angebot funktioniert, sich im Klaren sein, was man bei dessen Nutzung tut und die Folgen der eigenen interaktiven Handlungen abschätzen zu können.[127]

In diesem Kapitel werden Regeln vorgestellt, wie du Facebook überlegter nutzen und die wichtigsten Gefahren abwenden kannst. Die Methode „Versuch und Irrtum“ könnte mitunter folgenschwer sein, wenn zuerst in deiner Facebook-Chronik und später im Netz verfängliche Fotos kursieren, die lieber nicht kursieren sollten.

Kontinuierlich wird die Plattform umgebaut. Hast du die Grundstruktur und die Funktionsweise von Facebook verstanden, findest du dich schnell auch mit einer veränderten Oberfläche und mit neuen Funktionen zurecht.

Infos zu „Kinder im Netz“

http://www.noncaderenellarete.it
http://www.sicurinelweb.it
https://www.gianofamily.org
http://www.kinderserver-info.de

Tipp

Mithilfe eines Selbsttests kannst du herausfinden, wie das Werbeumfeld auf Facebook organisiert ist. Erstelle hierfür eine eigene Werbeanzeige und überlege, welche Produkte du verkaufen möchtest und suche dir die entsprechende Zielgruppe aus. Für die Werbeanzeige benötigst du ein Facebook-Konto, musst dich aber weder identifizieren noch eine Kreditkartennummer angeben. (www.facebook.com/ads/create)

126 Beim Börsengang im Mai 2012 war die Facebook-Aktie 38 Dollar wert und der Börsenwert von Facebook lag bei rund 104 Milliarden Dollar. Den aktuellen Kurs der Facebook-Aktie erfährst du z. B. hier: http://www.finanzen.net/aktien/facebook-Aktie. Zur Monetarisierung des Netzes: Maximilian Probst u. a. (2013): *Das Netz erstickt den Idealismus,* Zeit online, 17.10.2013 - 08:00 Uhr, http://www.zeit.de/2013/43/silicon-valley-usa-internetskepsis

127 Zum Boston-Attentat im April 2013 gab es ein „Twitter-Gewitter“ von mehr als 15 Millionen Tweets. Schnell verbreiteten sich Namen und Adresse samt Foto von mutmaßlichen Attentätern in den sozialen Medien. Die Web 2.0-Ermittlungsarbeit hat gezeigt, dass diese auch problematisch sein kann. Panikmache, Sensationslust und ungeprüfte Information nach dem Motto „Hast du schon gehört?“ können Unschuldige an den Pranger stellen: http://www.freitag.de/autoren/klaus-raab/warum-auch-serioese-medien-falsch-informieren. Ein Grundprinzip des rechtsstaatlichen Strafverfahrens besagt, dass eine Person bis zur rechtskräftigen Verurteilung als unschuldig gilt (Art. 27 II Verf.).

3.2 Facebook-Konto anlegen

Bevor wir uns mit den Funktionen von Facebook beschäftigen, legst du erst mal ein Facebook-Konto an, damit du die hier besprochenen Tipps leichter nachvollziehen kannst. Die Registrierung sollte wohlüberlegt erfolgen, weil es bereits hierbei um den Schutz der Privatsphäre geht.

Rufe zunächst die offizielle Webseite von Facebook auf.[128] Facebook fordert dich bei der Registrierung auf, Namen, E-Mail-Adresse, Geschlecht und Geburtsdatum anzugeben sowie ein Passwort festzulegen. Die Nutzungsbedingungen sehen vor, dass du dich mit dem „wahren Namen" registrierst, allerdings erfolgt keine Identitätsprüfung. Die Nutzer von Facebook müssen mindestens 13 Jahre alt sein. Die Überprüfung des Alters beschränkt sich jedoch nur darauf, nach dem Geburtsdatum zu fragen. In der Praxis ist es eine Frage der elterlichen Sorge, ob sie ihrem 12-jährigen Kind erlauben bei der Altersangabe zu schummeln.

Klarnamenzwang: Pro

- Klarnamen behindern die Trollkultur und fördern den guten Umgangston, weil die Nutzer später namentlich für ihr schlechtes Verhalten einstehen müssen.
- Klarnamen erschweren Stalking, üble Nachrede oder Beleidigungen, weil Täter einfacher identifizierbar sind.
- Klarnamen erleichtern die Ermittlungsarbeit der Fahnder.
- Klarnamen ermöglichen es Firmen, wie Facebook oder Google, über Surfprofile und individualisierte Werbung Geld zu verdienen.
- Eine offene, transparente Kultur des Diskurses erfordert ein „Vermummungsverbot" im Netz.

Willst du in Facebook unerkannt bleiben, solltest du dir überlegen, eine spezielle E-Mail-Adresse für Facebook zu verwenden. Die E-Mail-Adresse kannst du über eine der zahlreichen kostenlosen Maildienste erstellen.[129] Facebook erlaubt nämlich die Suche nach Facebook-Nutzern anhand ihrer E-Mail-Adresse. Verwendest du deine private oder geschäftliche E-Mail-Adresse bei Facebook, lässt sich einfach herausfinden, wer sich hinter einem bestimmten Profil verbirgt. Wähle ein sicheres Passwort für dein Facebook-Konto, das aus mindestens 16 Zeichen besteht und zusammengesetzt ist aus zufälligen Groß- und Kleinbuchstaben, Zahlen sowie Sonderzeichen.[130]

Hast du die geforderten Personendaten[131] eingegeben, wirst du in *Schritt 1* gebeten, den Zugriff auf dein

128 https://www.facebook.com/

129 Google Gmail: https://mail.google.com/; Microsoft Outlook.com: http://www.microsoft.com/de-de/outlook-com/; Yahoo Mail: https://de.mail.yahoo.com/

130 Sichere Passwörter kannst du mithilfe eines Passwortmanager generieren und verwalten. KeePass 2 (http://keepass.info/) ist ein Tool für PCs, KeePass2Android (https://play.google.com/store) ist eine App für Android-Smartphones.

131 Facebook sieht die Pflicht zum Klarnamen vor: http://www.facebook.com/legal/terms. Wer sich in sozialen Netzwerken unter fremder Identität einen Account mit dem Ziel anlegt, den Ruf des wirklichen Inhabers der Identität etwa durch üble Nachrede zu schädigen, sich mit Bekannten und Freunden des Opfers zu verlinken oder in dessen Namen Waren zu kaufen, begeht eine Straftat. Der Identitätsmissbrauch wird mit bis zu einem Jahr Freiheitsstrafe geahndet (Art. 494 c.p.).

E-Mail-Konto zu gewähren und dein persönliches Adressbuch bei Facebook hochzuladen. Facebook nutzt die Kontaktdaten dazu, einfacher Bekannte zu finden, die beim Netzwerk bereits angemeldet sind und außerdem dazu, Einladungsnachrichten an Nichtmitglieder zu versenden. Dem Zugang solltest du nicht zustimmen, weil sich deine Freunde, Bekannten oder Geschäftspartner über den Kontakt-Spam ärgern könnten und weil du Kontaktdaten nach dem italienischen Datenschutzkodex nicht ohne Einwilligung der Betroffenen weitergeben darfst. Bedenke, im Offline-Leben gibst du dein E-Mail-Passwort auch nicht aus der Hand. Klicke deshalb auf *Diesen Schritt überspringen*.

Überspringe auch *Schritt 2* und *Schritt 3*; Facebook fragt nach Schule, Hochschule, Arbeitgeber und Profilbild. Deine Profildaten kannst du später vervollständigen. Zum Abschluss der Registrierung bekommst du von Facebook eine E-Mail mit Link. Starte dein Mail-Programm und folge den Anweisungen in der E-Mail-Nachricht. Hast du alles erledigt, verfügst du über ein Facebook-Konto.

Klarnamenzwang: Contra

- Pseudonyme ermöglichen es Bürgerrechtlern in autoritären Staaten, Menschenrechtsverletzungen anzuprangern und gegen die Regierung zu opponieren.
- Pseudonyme ermöglichen es Außenseitern, unpopuläre Ideen zu diskutieren und sich vor einer intoleranten Mehrheit zu schützen.
- Pseudonyme ermöglichen, dass User mehrere Online-Identitäten wählen können: als Freund, Kunde, Gamer, eBayer und so weiter.
- Pseudonyme erleichtern es Gewaltopfern, Lesben, Schwulen, Transsexuellen, Essgestörten oder Lichternährern sich in Online-Foren freier auszutauschen.
- Kreative wählen u. a. Pseudonyme, weil sich ihre Werke darunter leichter vermarkten lassen.

Die Hausregeln von Facebook

Registrierst du dich bei Facebook, erklärst du dich mit den Nutzungsbedingungen der Plattform einverstanden. Ändert Facebook später die Nutzungsbedingungen, stimmst du den neuen AGB automatisch zu, indem du dich in dem sozialen Netzwerk einloggst. Eine Klausel in den Nutzungsbedingungen erlaubt allerdings Facebook, diese rückwirkend zu ändern.[132] Dies gibt Facebook große Freiheiten, die persönlichen Daten und Medieninhalte nach Belieben freizugeben.

Als Facebooker gewährst du der Plattform ein einfaches Lizenzrecht an allen eingestellten Inhalten.[133] Die einfache Lizenz ist erforderlich, damit Facebook die hochgeladenen Fotos speichern, kopieren, deinen Freunden anzeigen oder für personalisierte Werbung verwenden kann. Klickst du auf einer Produktseite auf

132 Proteste gegen Änderungen der Nutzungsbedingungen in der Facebook-Chronik sind rechtlich irrelevant. Wer juristisch wirksam einen Protest gegen Facebook ausüben möchte, muss diesen klassisch per Einschreiben mit Rückantwort vornehmen. Faktisch bleibt aber für unzufriedene Nutzer nur die Möglichkeit das Facebook-Konto zu löschen.

133 In der Facebook-„Erklärung der Rechte und Pflichten“ steht: „Du gibst uns eine nicht-exklusive, übertragbare, unterlizenzierbare, unentgeltliche, weltweite Lizenz für die Nutzung jeglicher IP-Inhalte, die du auf oder im Zusammenhang mit Facebook postest (‚IP-Lizenz‘). Diese IP-Lizenz endet, wenn du deine IP-Inhalte oder dein Konto löschst; es sei denn, deine Inhalte wurden mit anderen geteilt und diese haben die Inhalte nicht gelöscht.“ Der Profifotograf, der seine Fotos verkaufen will, sollte sich also reiflich überlegen, ob er seine Qualitätsbilder in Facebook einstellt. Facebook kann nämlich über seine Bilder frei verfügen – ohne sein Einverständnis und ohne Vergütungspflicht.

„Gefällt mir“, erhalten deine Facebook-Freunde eine „soziale Anzeige“, eventuell mit deinem Profilfoto. Facebook wertet nicht nur das Verhalten der Nutzer im sozialen Netzwerk aus, sondern auch die besuchten Internetseiten und die genutzten Apps. Wie funktioniert das? Technisch möglich ist dies über Cookies. Nutzer, die per Smartphone auf Facebook eingeloggt sind und auf einer Produktseite eines Fotofachgeschäftes auf „Gefällt-mir“-Buttons klicken, erhalten Werbeeinblendungen zu Kameras, Blitzgeräten oder Apps zur Bildbearbeitung. Ruft der Nutzer mit seinem PC dieselbe Produktseite noch einmal auf, kann er vom Werbetreibenden nicht wiedererkannt werden. Das entsprechende Cookie fehlt (noch) im Browser des PCs. Das Werbenetzwerk Atlas setzt hier an und verknüpft Informationen über verschiedene Endgeräte und Browser – sofern die Endgeräte Facebook bekannt sind. Wer also auf dem Smartphone nach Büchern zur Porträtfotografie recherchiert, sieht auf dem PC u. U. Buchwerbung zu Landschafts- oder Makrofotografie.

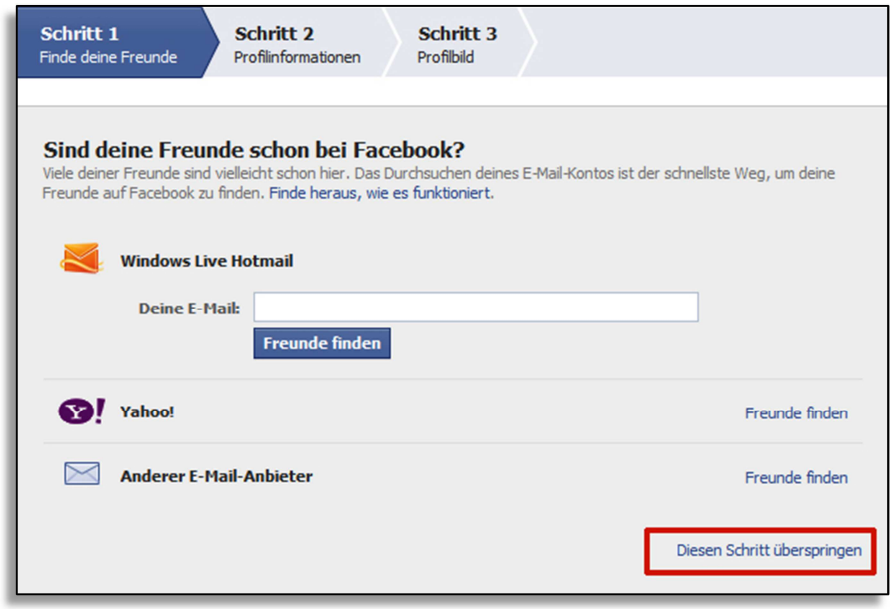


Abb. 17: Facebook-Zugriff auf das Adressbuch

Gibt es Möglichkeiten, die Datensammelei zu begrenzen? Ja, zum Teil durch Selbstschutz. Erstens, logge dich über den Browser Mozilla Firefox[134] mit Add-ons wie Ghostery[135] oder BetterPrivacy[136] bei Facebook ein. Zweitens, verwalte Anmeldungen auf externen Webseiten nicht per Facebook-Account. So verhinderst du, dass Facebook weiß, was dich außerhalb der sozialen Plattform interessiert.

3.3 Facebook-Funktionen

Bei Facebook werden die Funktionen ständig erweitert. So können Benutzer ein Profil anlegen, Statusmeldungen senden, chatten, mailen, Fotos und Videos hochladen, Interessen per „Gefällt-mir“-Button bekunden, in Gruppen kommunizieren, alleine oder mit Facebook-Freunden spielen, Ortsmarkierungen vornehmen, Freunde

134 https://www.mozilla.org/de/firefox/new/
135 https://addons.mozilla.org/de/firefox/addon/ghostery/
136 https://addons.mozilla.org/de/firefox/addon/betterprivacy/

markieren und nach Informationen suchen. Zu den zentralen Säulen des sozialen Netzwerks gehören die Chronik (Timeline) und das Newsfeed. Die Chronik enthält Informationen über die Aktivitäten des Profilinhabers und das Newsfeed ist der Nachrichtenticker über Neues bei Freunden.

Facebook-Chronik (Timeline)

Die Chronik ist die persönliche Seite auf Facebook, wo sich die Benutzer „Zur-Schau-stellen“. Hier schreiben die Benutzer, welchen Kaffee sie trinken, welchen Videoclip sie auf YouTube gesehen haben, was sie von der Filmmusik zu „Django Unchained“ halten, dass sie nun Single sind oder mit wem sie in den Urlaub fahren. Die geposteten Ereignisse, Statusmeldungen und Fotos werden in Form eines virtuellen Lebenslaufes protokolliert. Posten die Benutzer einen Inhalt, werden die Freunde via Newsfeed sofort darüber informiert. Diese können nun ihrerseits aktiv werden und die veröffentlichten Inhalte kommentieren oder auf den „Gefällt-mir“-Button klicken. So entsteht ein multimediales Tagebuch. Nutzer finden sich hierbei abwechselnd im Publikum und als Selbstdarsteller auf der Bühne wieder. Facebook funktioniert, weil „Freunde sehen, was Freunde machen“ und die Chronik ist hierzu die Informationszentrale.

> *„So unmittelbar wie gute werden auch schlechte Quellen gleichwertig in den Nachrichtenstrom eingespeist.“*
>
> Klaus Raab, Journalist

Abb. 18: Facebook Status-Update

Grundlage des persönlichen Netzwerkes bildet die „Freundesliste“. Über die Freundesliste unterhält der Benutzer Kontakte zu den anderen Mitgliedern. „Freunde“ sind bei Facebook Personen, zu denen der Benutzer einen Kontakt hergestellt hat. Dazu zählen neben den tatsächlichen Freunden auch Mitschüler, Berufskollegen sowie Bekannte und Verwandte.

Newsfeed

Über die Newsfeeds erfährt der Benutzer, was die Facebook-Freunde machen: wer was als Status-Update veröffentlicht hat, wer welche Fotos hochgeladen hat, welcher Freund ein neues Level in einem Spiel geschafft hat oder wer welche Web-Inhalte mit einem „Gefällt-mir“ bewertet hat. Newsfeed geben in Echtzeit Einblick über die Aktivitäten der Facebook-Freunde und laden zur Konversation ein.[137]

137 Mit „Facebook Home“ gelangen Nutzerdaten und Werbung unmittelbar auf den Startbildschirm von Android-Smartphones: http://www.zeit.de/digital/mobil/2013-04/facebook-home; http://www.zeit.de/digital/mobil/2013-04/facebook-home-apple-google

Mehrere Nachrichtenkanäle sorgen dafür, dass die Facebook-Freunde stets auf dem Laufenden sind. Freunde, die gerade online sind, sind mit einem grünen Punkt (im rechten unteren Teil) markiert. Klickt man auf deren Namen, ertönt beim Chat-Partner eine Glocke, die eine Chat-Anfrage signalisiert. Kleine rote Zahlen (im linken oberen Rand) zeigen an, dass neue Freundschaftsanfragen, Nachrichten oder Benachrichtigungen vorliegen. Schließlich sendet Facebook E-Mails an Benutzer, die über die Aktivitäten der eigenen Freunde informieren.

3.4 Wie schützt du deine Privatsphäre?

Bist du bei Facebook registriert, solltest du dir die erforderliche Zeit nehmen, um die Voreinstellungen deinen eigenen Interessen anzupassen. Facebook folgt nämlich dem sogenannten Opt-out-Prinzip und sieht grundsätzlich vor, dass alle Daten und Inhalte erstmals für alle sichtbar sind. Willst du aber, dass Bekannte ein bestimmtes Urlaubsfoto oder eine bestimmte Statusmeldung nicht sehen sollen, dann musst du aktiv werden. Letztlich musst du für dich entscheiden, welche Inhalte für wen sichtbar oder nicht sichtbar sind. Sollte der Schutz der Privatsphäre für dich ein wertvolles Gut auch in der vernetzten Welt sein, dann überlege zweimal, bevor du private und pikante Inhalte auf Facebook postest, was du mit Freunden von Freunden oder Unbekannten teilst, welche Person du auf Facebook sein willst. Wo liegt die richtige Balance zwischen Selbstkontrolle und Selbstdarstellung? Eine offene Frage. Abwägen kann aber nur derjenige Nutzer, der die Optionen kennt.

Die nächsten Abschnitte informieren darüber, wie du deine Privatsphäre auf Facebook schützen kannst. Manche Klickpfade können schnell veraltet sein. Facebook erneuert seine Webseite ständig; einmal geht es um neue Funktionen, ein anderes Mal um ein erneuertes Design. Findest du die Facebook-Einstellungen nicht auf Anhieb, solltest du zu deiner speziellen Frage eine Web-Recherche machen oder eine Anfrage in den einschlägigen Foren stellen.

3.4.1 Das Profil – Das virtuelle „Ich“

Wer Facebook nutzen will, muss sich mit einem persönlichen Profil registrieren. Das Profil ermöglicht den Blick auf das „ganze Leben“ des Benutzers. Darin liegt das Grundproblem bei Facebook. Du kannst, wenn du willst, dich auf Facebook zu einem gläsernen Nutzer machen und wahrheitsgemäß deine Hobbys, Lieblingsfilme sowie Daten zur Schule, zum Arbeitsplatz, zum Beziehungsstatus und deine Kontaktinformationen angeben.

Andererseits kannst du dein Profil so aufmotzen, dass du möglichst viele Freunde gewinnst und möglichst viele „Likes“ erhältst. Die Zahl der „Freunde“ und der „Likes“ ist dann gewissermaßen der Kurswert des Profils. In diesem Fall muss das Profil ständig aktualisiert werden, um zeitgeisttauglich zu sein oder - in der Börsensprache - um den „schnellen Gewinn“ abschöpfen zu können. Überlege gut, ob du dich auf Facebook so darstellst, wie du im „richtigen Leben“ wirklich bist, ob dir die „Kurswerte“ wichtig sind oder ob es Privates gibt, das für andere tabu ist.

In deinem Profil kannst du viel über dich preisgeben: Wohnort, Interessen, religiöse und politische Ansichten. Gehe zurückhaltend mit deinen Daten um; muss Facebook alles über dich wissen? Gibst du deine Anschrift an, sollte sie grundsätzlich nie für alle Nutzer einsehbar sein. Wer dich aus der Schule oder vom Arbeitsplatz kennt, weiß sowieso, wo du wohnst. Will ein Nutzer deinen Wohnort oder deine E-Mail-Adresse wissen, kann er dazu eine Anfrage stellen und du entscheidest im konkreten Fall, ob du diese Infos preisgibst oder nicht. Zudem verringerst du das Risiko, dass deine Kontaktdaten in falsche Hände geraten. Mit wenigen Klicks kannst du deine Kontakt- und Profilinformationen ausblenden. So geht’s: Klicke auf deinen Facebook-Namen und drücke auf die Schaltfläche *Info*. Im nächsten Fenster kannst du bei jedem Abschnitt festlegen, welcher Nutzerkreis die persönlichen Daten sehen kann. Deinem Arbeitgeber gehen deine politischen Einstellungen nichts an. Oder du kannst beispielsweise festlegen, dass Bücher, die dir gefallen, nur ein bestimmter Kontakt sehen kann, deine Hobbys nur deine Freunde sehen können.

Tipp

Nutze nach jeder Einstellungsänderung die Vorschau-Funktion. Mit dem Ansichtscheck kannst du überprüfen, was andere Personen, etwa deine letzte Urlaubsbekanntschaft, mit eingeschränkten Rechten von deinem Profil sehen kann.

„Mir gefällt das mit den Bildern nicht besonders, aber meine Schwester lädt tonnenweise Photos hoch. Schon ihre Profilbilder verraten einem alles über sie, und in ihren Photoalben findet man alle Typen, mit denen sie mal was hatte. Das finde ich echt nicht mehr normal.“

Daniel Miller, Ethnologe

3.4.2 Privatsphäre-Einstellungen anpassen

Wie kannst du deine Facebook-Daten schützen? Du musst die verschiedenen Möglichkeiten kennen, mit denen du die eigenen Einstellungen zur Privatsphäre anpassen kannst. Die Wahl hat nur der, der die Alternativen kennt. Beherzige die folgenden Tipps, dann wirst du nicht nach Jahren vielleicht kopfschüttelnd auf deine Posts bei Facebook zurückschauen. Klar sollte aber auch sein, dass strenge Privatsphäre-Einstelllungen die eigenen Inhalte nur vor den Augen anderer Nutzern verbergen, aber nicht vor der Firma Facebook.

Wer kann dich finden?

Standardmäßig können Facebook-Nutzer dich über die E-Mail-Adresse oder Telefonnummer finden, die du bei der Registrierung hinterlegt hast. Willst du auf Facebook nicht so ohne weiteres gefunden werden, dann wähle zunächst eine E-Mail-Adresse, die du nur für Facebook nutzt. Unter *Privatsphäre-Einstellungen und Werkzeuge* kannst du festlegen, wer nach dir suchen kann. Zur Auswahl stehen *Alle*, *Freunde von Freunden* und *Freunde*. Wählst du die Option *Freunde* aus, kannst du über die E-Mail-Adresse und Telefonnummer nur *von* deinen aktuellen Facebook-Freunden gefunden werden.

Außerdem hast du hier die Möglichkeit, deine Facebook-Chronik vor Google & Co. zu verbergen. Willst du nicht, dass Suchmaschinen den Link zu deiner Chronik in ihren Suchergebnissen anzeigen und dein Profil somit im Internet auffindbar ist, dann entferne das Häkchen vor der Option *Anderen Suchmaschinen das Verlinken auf deine Chronik gestatten*.

Tipp

Mit einer Web-Suche kannst du das öffentliche Profil von Facebook-Nutzern finden. So geht's: „<Vorname Nachname> site:facebook.com"

Wer kann dich kontaktieren?

Hast du kein Interesse an einer großen Freundesschar, kannst du einschränken, von wem du Freundschaftsanfragen erhältst. Rufe dazu die *Privatsphäre-Einstellungen und Werkzeuge* auf und klicke neben *Wer kann mich kontaktieren?* auf *Bearbeiten* und wähle aus der Dropdown-Liste die Option *Freunde von Freunden*.

Überprüfe Freundschaftsanfragen

Ohne Freunde macht Facebook wenig Sinn. Wer ein soziales Netzwerk aufbauen möchte, muss über Freundschaftsanfragen neue Kontakte knüpfen. Wer steckt hinter einer unscheinbaren Anfrage? Es kann sich um Kriminelle mit gefälschten Konto („Fake-Account") handeln, die dich auf manipulierte Webseiten locken wollen, Viren auf deinem Smartphone verbreiten wollen und lediglich Interesse an deinen Bankdaten haben. Unbekannte solltest du nicht so ohne Weiteres in deine Kontaktliste aufnehmen. Wie kann man aber die „guten" von den „bösen" Anfragen unterscheiden? Hinweise für ein gefälschtes Facebook-Konto sind: „freizügiges" Profilfoto, Links zu zweifelhaften Webseiten oder Anwendungen und sehr viele Freunde. Erkundige dich im Internet nach der Vertrauenswürdigkeit der Anfrage. Du kannst auch höflich zurückschreiben „Kennen wir uns?" und dir den Kontaktwunsch auch per Nachricht begründen lassen. Hast du Zweifel über die Identität und Motivation des Anfragenden, lehne die Freundschaftsanfrage ab. Erscheint ein neuer Freund erst im Nachhinein als dubios, kannst du dich schnell wieder „entfreunden". Gehe auf das Profil der entsprechenden Person, klicke rechts vom Button *Freunde* auf das kleine Dreieck. Im geöffneten Menü findest du den Eintrag *Als FreundIn entfernen*. Mit einem Klick darauf ist die Freundschaft aufgekündigt.

Regle die Sichtbarkeit der Inhalte und der Kontaktinfos

Auf Facebook kannst du dich mit deinen tatsächlichen Freunden, mit Bekannten oder auch mit fremden Personen vernetzten. Über Listen kannst du deine Kontakte in Gruppen aufteilen und Inhalte nur für die Personen in bestimmten Listen freigeben. Der Nutzer kann beispielsweise nur mit seiner Familie Fotos der letzten Familienfeier teilen.

Die Listen sind auf der Facebook-Startseite links vom Nachrichtenstrom zu sehen. Klicke auf *FREUNDE*, dann kannst du mit dem Button *+Liste erstellen* eine neue Freundesliste erstellen. Nun kannst du einen Namen für die Liste vergeben und die gewünschten Kontakte der Liste hinzufügen. Abschließend klicke auf *Erstellen*. Eine besondere der bereits vorhandenen Listen ist die Liste *Eingeschränkt*. Kontakte, die du dieser Liste zuordnest, sehen nur öffentliche Inhalte von dir. Geeignet ist diese Liste für flüchtige Bekanntschaften. Deine Kontakte erfahren von Facebook allerdings nicht, welchen Listen sie von dir zugeordnet wurden. Ebenso bleiben deine angelegten Listen vor anderen Facebook-Nutzern verborgen.

Reichweite der Inhalte

Beachte, dass deine geposteten Inhalte eine beachtliche Reichweite erlangen können. Hast du 150 Freunde, die ihrerseits auch 150 Freunde haben, bedeutet dies, dass deine veröffentlichten Inhalte potentiell 22.500 Personen sehen können!

Tipp

Du kannst deine Freundesliste verbergen, aber nicht verhindern, dass du in der Freundesliste deiner Freunde gelistet wirst. Willst du das nicht, musst du deine Freunde überzeugen, dass auch sie ihre Freundeslisten auf „unsichtbar“ umstellen.

Wer kann künftige Posts sehen? Standardmäßig ist bei Facebook erst mal alles öffentlich. Das heißt, alle Kontakte sehen deine Posts. Du kannst die Sichtbarkeit der Beiträge auch einschränken. Die Schaltzentrale dafür sind die *Privatsphäre-Einstellungen und Werkzeuge*. Hier kannst du festlegen, wer deine künftigen Beiträge sehen kann. Wähle die Option *Freunde*, denn dies verhindert versehentliche öffentliche Postings. Willst du einmal ein Foto öffentlich machen oder nur für eine bestimmte Freundesliste sichtbar, kannst du dies manuell direkt beim Posting festlegen. Die Auswahl *Benutzerdefiniert* dient dazu, die Inhalte vor bestimmten Personen du oder ganzen Listen zu verbergen. Postest du in einem anderen Profil, dann bestimmt der Inhaber jenes Profils, was andere von deinen Inhalten sehen können.

Freundesliste verbergen

Die Freundesliste ist standardmäßig für alle Nutzer sichtbar. Aber vielleicht möchtest du nicht, dass jeder, der sich dein Profil ansieht, auch deine Freundesliste sehen kann. Willst du die Sichtbarkeit der Freundesliste begrenzen, muss die Privatsphäre entsprechend bearbeitet werden. So geht’s: Klicke zunächst in der Menüleiste auf deinen Facebook-Namen, dann auf *Info*. Scrolle zum Abschnitt *Freunde* und klicke auf das kleine *Stift-Symbol*. Wähle im Drop-Down-Menü *Privatsphäre bearbeiten* und im nächsten Fenster kannst

du festlegen, wer deine Freundesliste sehen kann. Willst du eine Freundesliste gänzlich verbergen, dann wähle die Option *Nur ich*.

Poste überlegt

Die Chronik ist die Informationszentrale bei Facebook. Dort teilen Nutzer per Statusmeldungen, Fotos, Videos und Links vieles von sich mit. Überlege am besten zweimal, ob du etwas auf Facebook posten willst oder nicht. Soll wirklich jeder Beitrag für alle Facebook-Freunde sichtbar sein? Befinden sich unter deinen Kontakten auch Personen, die nicht jedes Detail aus deinem privaten Leben wissen sollten? Hat die Hauskatze eine Magenverstimmung, verfasst manche Katzenliebhaberin schon mal in einem traumatisierten Zustand eine unbedachte Statusmeldung. Möglicherweise bereust du am nächsten Tag, was du in der Stunde der Bitternis alles auf Facebook preisgegeben hast; die Statusmeldung dreht aber ihre Kreise: sie wurde in den letzten 6 Stunden bereits 78 Mal „gelikt“. Sei auch vorsichtig beim Posten von Fotos und Videoclips, auf denen andere Personen zu sehen sind. Deine Freunde und Bekannten möchten vielleicht nicht, dass Fotos von der vielzitierten feucht-fröhlichen Party in Facebook und später im Netz kursieren. Alles, was du bei Facebook postest und öffentlich zugänglich ist, kann kopiert werden und unkontrolliert im Netz vagabundieren. Bedenke, dass die abgebildeten Personen ein „Recht auf Bildnis“ haben. Das bedeutet, dass du, willst du ein Foto von ihnen auf Facebook hochladen, vorher ihre Einwilligung einholen musst(Artt. 12, 24, 96 I L 633/1941).

Tipp

Halte deine Urlaubspläne vor der Facebook-Öffentlichkeit geheim. Informierst du etwa „alle“ darüber, dass du vom 21. Juli bis 4. August nach Andalusien fährst, könnten Kriminelle solche Informationen für ihre Pläne ausnutzen.

Im Ernstfall kannst du eigene unbedachte Status-Meldungen oder peinliche Kommentare anderer Nutzer aus deiner Chronik entfernen. Suche dazu in der Chronik den Eintrag aus, den du löschen willst, klicke auf das kleine Stift-Symbol und dann noch zwei Mal auf *Löschen*.

Lege fest, wer in deine Chronik schreiben darf

Die Chronik ist ein (halb-)öffentlicher Ort auf Facebook; früher hieß sie Pinnwand. In der Chronik sieht man, was auf der Bühne des Nutzers „gespielt“ wird. Dort zeigt der Nutzer seine Interessen und Posts, aber auch andere können dort etwa Geburtstagsgrüße, Fotos oder Links hinterlassen. Es kann aber auch der Fall eintreten, dass bestimmte Freunde regelmäßig sehr ärgerliche Kommentare in deiner Chronik hinterlegen. Vor solchen Einträgen kannst du dich schützen, indem du ihren Zugriff auf deine Chronik verhinderst. Wie’s geht? Gehe zu *Chronik und Markierungseinstellungen*. Unter *Wer kann Inhalte zu meiner Chronik hinzufügen* kannst du über die Buttons *Bearbeiten* die Einschränkungen vornehmen. Im selben Fenster kannst du

auch die Beiträge, in denen du namentlich erwähnt wirst, überprüfen, bevor sie in deiner Chronik erscheinen. Die Chroniküberprüfung solltest du in jedem Fall aktivieren, denn nur so bleibst du Programmdirektor deiner Chronik.

Fotos entfernen lassen

Fotos, die deine Freunde hochgeladen haben, kannst du nicht entfernen. Wenn du nicht möchtest, dass Fotos, auf denen du in einer kompromittierenden Situation zu sehen bist, weiter online sind, stehen dir zwei gangbare Wege offen: Löschaufforderung oder Anwalt/Polizei einschalten.

Post- und Kommunikationspolizei
Reschenstraße 190
39100 Bozen
E-Mail: sez.polposta.bz@pecps.poliziadistato
Tel.: 0471/531411/19/16/13 oder 0471/531512

Erster Weg: Bitte deinen Freund das Foto wieder zu entfernen. Richte die Löschaufforderung per E-Mail oder über die Facebook-Funktion *Nachricht senden* und nicht über die Kommentarfunktion unterhalb des Bildes. Die Kommentarfunktion könnte erst recht jene Aufmerksamkeit hervorrufen, die du eigentlich vermeiden wolltest. Setze dem Freund unmissverständlich eine klare Frist, wie „innerhalb von 2 Tagen“ und mache vom umstrittenen Foto einen Screenshot. Kommt es doch zu rechtlichen Auseinandersetzungen, dann hast du den Fall dokumentiert. Wie man einen Screenshot macht, hängt von deinem Betriebssystem ab.

Zweiter Weg: Bei schwerwiegenden und dringlichen Fällen solltest du einen Anwalt einschalten oder eine Strafanzeige bei der Post- und Kommunikationspolizei erstatten.

Markierungen verwalten

In Facebook kannst du Personen auf Fotos namentlich zuordnen. Markierte Fotos sind dann mit dem entsprechenden Facebook-Profil verknüpft. Bist du auf einem Foto markiert, kannst du die Markierung im Nachhinein manuell entfernen. Gehe hierzu auf das Foto und klicke neben dem eigenen Namen auf *Markierung entfernen*. Im *Aktivierungsprotokoll* kannst du sehen, wer dich auf welchen Fotos markiert hat.

Sollen deine Kontakte zu deiner Person keine Markierungsvorschläge sehen, musst du zu *Chronik und Markierungseinstellungen* navigieren. Unter *Wer kann Markierungsvorschläge sehen, wenn Fotos hochgeladen werden, die dir ähneln?* wählst du mit dem Button die Option *Niemand.*

Wo befindest du dich?

Mit der Ortungsfunktion *Orte* können Nutzer bei jedem Status-Update angeben, wo sie sich gerade befinden. Haben sich Nutzer an einem Ort „eingecheckt“, erhalten ihre Freunde darüber eine Statusnachricht. Das

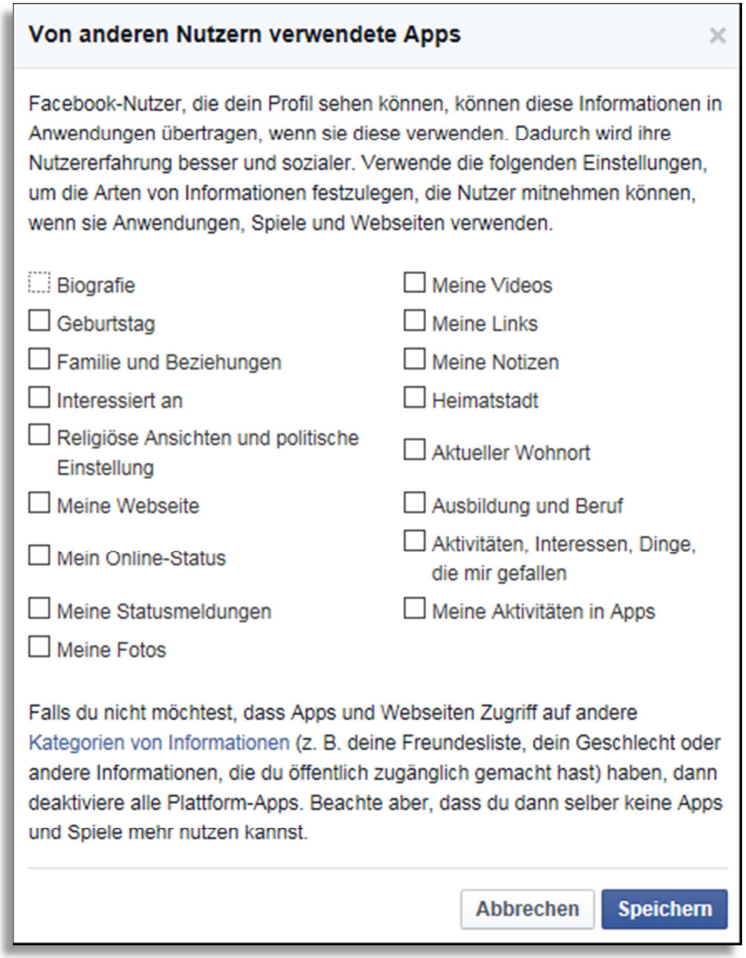
Tauschgeschäft der Ortungsfunktion besteht darin, dass Nutzer sich kurzfristig zu einem Kaffee in der Bahnhofsbar verabreden können, Facebook im Gegenzug Ortsdaten der Nutzer erhält und diese an die Werbekunden verkauft. Die Werbekunden können dann ortsbezogene Werbeanzeigen schalten, etwa zu aktuellen Sonderangeboten in der Bahnhofsboutique.

Problematisch an der Ortungsfunktion ist, dass Nutzer, ohne vorherige Zustimmung ihrer Freunde per Smartphone angeben können, an welchen Orten sich ihre Freunde gerade aufhalten. Willst du nicht, dass deine Freunde dich ohne deine vorherige Einwilligung auf Schritt und Tritt tracken können, musst du diese Funktion im Facebook-Profil über dein Smartphone deaktivieren.

Vorsicht bei Apps

Auf Facebook findest du auch Apps von Drittanbietern. Facebook selbst übernimmt keine Verantwortung für die App-Anbieter. Installierst du eine App, wirst du gefragt, auf welche Daten sie zugreifen darf. Ein Geburtstagskalender muss deinen Geburtstag kennen, eine Taxi-App deine Standortdaten, ein Gewinnspiel benötigt diese Daten nicht. Jede App hat auch AGBs (Allgemeine Geschäftsbedingungen) und Datenschutzrichtlinien. Du solltest dir Zeit nehmen und diese Angaben sorgfältig durchlesen. Nur so kannst du wissen, was mit deinen Personendaten passiert. Ohne dein Zutun greifen Apps auf Informationen zu, die für alle sichtbar sind und hinterlassen Nachrichten in deiner Chronik. Um dies zu unterbinden, musst du App-Nachrichten blockieren. Klicke dazu in einer solchen Nachricht oben rechts auf das *Kreuz* und wähle dann den Punkt *Sperren*.

Apps können selbst dann Daten über dich sammeln, wenn du sie nicht selbst verwendest, sondern wenn sie deine Freunde nutzen. Willst du die Weitergabe der Inhalte und Kontaktdaten an solche Apps einschränken, musst du die *App-Einstellungen* aufrufen. Gehe dann zum Abschnitt *Von anderen Nutzern verwendete Apps* und klicke auf den Button *Bearbeiten*. Entferne die Häkchen von allen Profildaten, auf die Apps von anderen Nutzern keinen Zugriff haben sollten (vgl. Abb. 19).


Von anderen Nutzern verwendete Apps
Facebook-Nutzer, die dein Profil sehen können, können diese Informationen in Anwendungen übertragen, wenn sie diese verwenden. Dadurch wird ihre Nutzererfahrung besser und sozialer. Verwende die folgenden Einstellungen, um die Arten von Informationen festzulegen, die Nutzer mitnehmen können, wenn sie Anwendungen, Spiele und Webseiten verwenden.
Biografie
Geburtstag
Familie und Beziehungen
Interessiert an
Religiöse Ansichten und politische Einstellung
Meine Webseite
Mein Online-Status
Meine Statusmeldungen
Meine Fotos
Meine Videos
Meine Links
Meine Notizen
Heimatstadt
Aktueller Wohnort
Ausbildung und Beruf
Aktivitäten, Interessen, Dinge, die mir gefallen
Meine Aktivitäten in Apps
Falls du nicht möchtest, dass Apps und Webseiten Zugriff auf andere Kategorien von Informationen (z. B. deine Freundesliste, dein Geschlecht oder andere Informationen, die du öffentlich zugänglich gemacht hast) haben, dann deaktiviere alle Plattform-Apps. Beachte aber, dass du dann selber keine Apps und Spiele mehr nutzen kannst.
Abbrechen
Speichern
Abb. 19: Zugriffsrechte der Apps

3.5 Rechtliches für Inhalte in Facebook

3.5.1 Urheber- und Persönlichkeitsrecht

Facebook ist auch ein öffentlicher Raum, in dem Rechtsregeln gelten. So darf man nicht nach Herzenslust Inhalte posten oder sharen. Worauf musst du achten, damit du dir keinen rechtlichen Ärger einhandelst? Wer geschützte Inhalte ohne Erlaubnis des Urhebers oder Rechteinhaber auf Facebook zugänglich („Freunden von Freunden“) macht, riskiert, dass sein Konto gesperrt wird. Und schließlich sollte man sich fragen, ob man Facebook wirklich eine einfache Nutzungslizenz für die veröffentlichten Werke einräumen möchte.

Was ist bei Fotos zu beachten?

Fotos von anderen Menschen dürfen nur mit deren Einwilligung auf Facebook hochgeladen werden. Bei Kinderfotos ist auch die Einwilligung der Eltern erforderlich. Eine Einwilligung ist entbehrlich, wenn die Personen als Beiwerk auf der Aufnahme erscheinen, bei Fotos von Versammlungen oder bei Personen aus dem Bereich der Zeitgeschichte, wie Manager, Politiker oder Schauspieler. Bei Fotos können auch Rechte des Fotografen im Spiel sein. Fotos, die eine minimale schöpferische Leistung aufweisen, unterliegen dem Urheberrecht. Das bedeutet, dass Nutzer, die auf Facebook ohne Zustimmung des Fotografen Fotos veröffentlichen, damit rechnen müssen, dass eine kostspielige Abmahnung ins Haus flattert.

Dürfen Schüler die Chemie-Formelsammlung per Handy von der Schultafel oder vom Arbeitsblatt eines Chemiebuches abknipsen und auf Facebook online stellen? Im Fall des Chemiebuches droht Ärger, weil der Verlag wegen Urheberrechtsverstoßes abmahnen kann. Und was passiert, wenn Freunde auf die Chronik die Formelsammlung posten und Urheberrecht verletzen? Informiert der Verlag den Schüler über den rechtswidrigen Inhalt in seiner Chronik und verlangt, die Formelsammlung von der Seite zu entfernen, muss er dies unverzüglich tun.

Fotos können jederzeit kopiert, weiterverbreitet oder in einen unerwünschten Kontext gestellt werden. Bei allzu freizügigen Bildern sollte das mitbedacht werden.[138] Muss das Foto unbedingt markiert werden? Wird Software zur automatischen Gesichtserkennung eingesetzt, kann diese mit großer Trefferquote alle Fotos erkennen, auf denen der Markierte abgebildet ist. Sind die Fotos zudem mit Geotags versehen, kann auch der Standort der Fotos ermittelt werden. Verzichte aufs Geotagging bei Fotos, die du ins Netz stellst.

138 Die App Confide bietet die Möglichkeit, verschlüsselte Fotos an andere Confide-User zu versenden und löschen zu lassen, ohne dass der Empfänger davon Screenshots machen kann. Webseite des Entwicklers: https://getconfide.com/

Enthalten Fotos in sozialen Netzwerken keine Daten zum Aufnahmeort, können sie auch nicht in falsche Hände gelangen.

Darf man fremde Videos einbetten?

Gängige Praxis auf Facebook ist, auf YouTube Videos zu verlinken. Dabei bindet Facebook den YouTube-Player ein mit der Folge, dass der Nutzer zum Weiterverbreiter des YouTube-Videos wird. Die Frage ist, ob man Videos in Facebook einbetten darf. Der EuGH[139] hat entschieden, dass „framende Links“ das Urheberrecht nicht verletzen. Bietet also der Anbieter des YouTube-Videos den Share-Button an, gewährt er damit das Recht, das Video auf Facebook zu teilen. Der Facebook-Nutzer kann davon ausgehen, dass der Anbieter des Videos die Rechte am Video innehat. Ist das nicht der Fall, droht nur dem Anbieter des Videos auf YouTube Ärger, aber nicht dem Facebook-Nutzer.

Darf man fremde Texte veröffentlichen?

Eigene Texte kannst du nach Belieben veröffentlichen. Fremde Texte dürfen nur mit Zustimmung des Autors oder des Rechteinhabers (Verlag) verbreitet werden. Hingegen darf man aus fremden Werken ohne Erlaubnis zitieren, vorausgesetzt, das Zitat, als solches gekennzeichnet, ist nur Beiwerk eines eigenständigen Werkes und dient der geistigen Auseinandersetzung – so die Vorgaben des Urheberrechts. Die Praxis sieht anders aus. Es werden einfach Zitate gepostet, ohne Quellangaben und ohne eigene Kommentare. Sind fremde Werke nur Facebook-Freunden zugänglich, besteht ein geringes Risiko, dass die Rechteinhaber Kenntnis von der Rechtsverletzung erhalten. Erfahren Rechteinhaber von der rechtswidrigen Veröffentlichung ihrer Inhalte, kann rechtliches Ungemach drohen.

Was muss man bei eigenen Inhalten beachten?

Selbst erstellte Inhalte, wie Texte, Fotos, Videos können Nutzer nicht so ohne weiteres auf Facebook veröffentlichen. Zu achten ist darauf, ob dabei fremde Rechte verletzt werden. Lädst du beispielsweise eigene Handyvideos von Konzerten auf Facebook hoch, verletzt du Urheberrecht. Die Veranstalter von Konzerten verbieten in der Regel das Verbreiten von Live-Mitschnitten. Selbst geknipste Fotos der Sonderausstellung einer Künstlervereinigung, die auf Facebook eingestellt werden, verstoßen gegen das Urheberrecht. Die Künstlervereinigung will nämlich über den Verkauf des Ausstellungskatalogs einen Teil ihrer Ausstellungskosten decken.

139 EuGH C-348/13 Beschluss vom 21.10.2014: http://curia.europa.eu/juris/liste.jsf?num=C-348%2F13

3.5.2 Impressumspflicht

Wann ist ein Impressum in Facebook Pflicht? Ein Impressum wird nur für geschäftsmäßige Web-Auftritte benötigt. Dazu zählen solche Web-Angebote, bei denen eigene oder fremde Produkte beworben werden, die eigene Firma dargestellt wird sowie Facebook-Fanseiten. Aber auch für persönliche Facebook-Profile, die nicht für rein private Zwecke genutzt werden, ist ein Impressum Pflicht, etwa wenn ein Musiker in der Chronik auf seine Konzerttermine hinweist. Ein Impressum soll Transparenz über die Identität des Anbieters schaffen. Für Kunden ist maßgeblich, an wen sie sich im Falle einer Reklamation wenden können.

Welche Daten gehören ins Impressum? Ins Impressum gehören immer Name, Anschrift sowie E-Mail-Adresse, PEC-Adresse und Telefonnummer des Anbieters. Die weiteren Pflichtangaben hängen vom Beruf sowie von der Rechtsform der Firma des Anbieters ab.

Wie muss das Impressum gestaltet sein? Der Gesetzgeber fordert, dass Nutzern die Anbieterkennzeichnung in „leicht erkennbarer und unmittelbarer Weise“ zugänglich sein muss. Der Anbieter kann auf der Facebook-Seite auch auf das Impressum seiner eigenen Webseite verlinken. Der Link muss aber eine eindeutige Bezeichnung wie „Impressum“ oder „Kontakt“ aufweisen. Der Textlink „Info“ reicht nicht aus, weil der durchschnittliche Besucher dahinter kein Impressum vermuten würde.

3.6 Umgang mit Cybermobbing

Zur Web 2.0-Generation gehört zu chatten, zu teilen, von unterwegs Fotos und Videos aufzunehmen und sofort auf soziale Netzwerke zu posten. Für viele Jugendliche sind soziale Netzwerke ein Instrument der freien Persönlichkeitsentfaltung, ein Teil nutzt sie für wiederholte Beleidigungen und Spott. Das vermeintlich anonyme Internet senkt offenbar die Hemmschwelle für Mobbing. Klären wir zunächst, was Cybermobbing von einem harmlosen Streit unterscheidet und zeigen dann auf, wie sich Opfer wehren können.

3.6.1 Was ist Cybermobbing?

Von Cybermobbing spricht man, wenn „ein Opfer über einen längeren Zeitraum per (Online-)Medien schikaniert und gedemütigt wird.“[140] Beleidigungen können auf Facebook veröffentlicht, entwürdigende Videos auf

140 Wilfried Schubarth (2010): *Neue Gewalt- und Mobbingphänomene als Herausforderung für Schulen,* in: APuZ 38/2010, S. 27, http://www.bpb.de/apuz/32513/kinderrechte

YouTube hochgeladen oder Gemeinheiten rund um die Uhr per SMS versendet werden. Einmal ins Netz gestellte Fotos oder Videos können sich schnell verbreiten und unkontrolliert gespeichert werden; Mobbing-Inhalte können auch nach drei oder zehn Jahren wieder an die Öffentlichkeit gelangen; das Internet vergisst nicht. Mobber können anonym handeln, weil sie vielfach ihre Angriffe über ein Fake-Profil durchführen.

Cybermobbing kann in unterschiedlicher Art und Weise erfolgen; es kann von der Beleidigung in Foren oder sozialen Netzwerken, über das Verbreiten von Gerüchten, um darüber etwa Freundschaften zu zerstören, wiederholte anonyme Anrufe per Handy, Veröffentlichung privater Aufnahmen, um den Ex-Partner zu blamieren, bis zur Androhung von Gewalt reichen. Nicht jede Bloßstellung ist allerdings mit einer bösen Absicht verbunden, sie kann auch nur aus Spaß erfolgen. Dumme Scherze können sich aber zum Mobbing entwickeln, wenn sie fortwährend erfolgen. Peter Koler, Direktor vom Forum Prävention der Provinz Bozen, weist darauf hin, dass Mobbing weitreichende negative Folgen für die Gesundheit und für die soziale Situation des Betroffenen haben kann. Mobbing-Opfer „leiden unter Beschwerden wie Kopf-, Rücken-, Bauchschmerzen oder Schlafstörungen. Gemobbte schätzen ihre eigene Leistungsfähigkeit häufig schlechter ein, sind unzufriedener mit ihrem Aussehen, verbringen seltener Zeit mit Freunden und greifen als Bewältigungsstrategie eher zu Zigaretten, Alkohol oder anderen Drogen.“[141]

Ist Cybermobbing strafbar?

In Italien gibt es derzeit kein spezielles Cybermobbing-Gesetz. Wer andere beispielsweise in Facebook oder per SMS beschimpf, bloßstellt, „zur Strecke bringt“, muss unter Umständen mit strafrechtlichen Konsequenzen rechnen. Aspekte des Cybermobbings können aber mit bestehenden Gesetzen geahndet werden:

- Beleidigung (Art. 594 c.p.): Eine Beleidigung begeht derjenige, der die persönliche Ehre und Würde eines anderen durch „Schriften oder Abbildungen“ verletzt. Eine Beleidigung kann mit einem Kommentar wie „Pornoqueen“, „Schmarotzer“, „Bettnässer“ in der Facebook-Chronik erfüllt sein.
- Rufschädigung (Art. 595 c.p.): Eine Rufschädigung begeht der, wer trotz besseres Wissen unwahre, ehrenrührige Tatsachen behauptet und verbreitet. Der Täter weiß, dass er lügt, wenn er etwa sagt „Der Beamte XY ist bestechlich“ oder die „Die Firma XY verkauft abgelaufene Lebensmittel“.
- Stalking (Art. 612-bis c.p.): Stalking liegt vor, wenn eine Person einer anderen Person beharrlich nachstellt und diese ständig belästigt. Das kann etwa durch Posten von anzüglichen Fotos sein, durch unentwegte „Liebesbezeugungen“ auf der Pinnwand von Freunden oder durch Zusenden von E-Mails zu allen Tages- und Nachtzeiten.

141 http://www.forum-p.it/de/news/109.html, letzter Zugriff: 02.08.2013

- Recht am eigenen Bild (Art. 96 L 633/1941): Das Recht am eigenen Bild besagt, dass Fotos von Personen nur mit Erlaubnis der Abgebildeten verbreitet werden dürfen. Es ist also nicht erlaubt, Mitschüler oder Lehrer während des Unterrichts ohne ihr Einverständnis zu fotografieren und beispielsweise auf die Fotoplattform Flickr hochzuladen. Wer hingegen eine Fotomontage verbreitet, in der das Gesicht der Ex-Freundin mit einem pornografischen Bild zusammengesetzt ist, begeht eine Straftat (Artt. 615-bis, Art. 617-sexies c.p.).
- Identitätsdiebstahl (Art. 494 c.p.): Ein Identitätsdiebstahl liegt vor, wenn ein Mobber unter dem Namen des Opfers ein Benutzerkonto anlegt und darüber Beleidigungen oder peinliche Fotos und Videos verbreitet. Die Freunde des Opfers müssen hierbei den Eindruck haben, dass die Mobbing-Inhalte vom Opfer selbst stammen. Der Identitätsdiebstahl ist strafbewehrt und wird mit Freiheitsstrafe bis zu einem Jahr geahndet.

Facebook-Nutzer, welche die rechtlichen Rahmenbedingungen ihres Handelns kennen, sind besser davor geschützt, durch unbedachtes Handeln straffällig zu werden.

3.6.2 Schutz vor Cybermobbing

Vorbeugen

Wie kann man sich wirksam vor Cybermobbing schützen? Ein guter Schutz ist ein freundlicher Umgangston und Gelassenheit bei Konflikten. Beherzigst du zudem ein paar Grundregeln in sozialen Netzwerken, verringert sich das Risiko ein Mobbing-Opfer zu werden.

- Schütze deine Inhalte: Passe deine Privacy-Einstellungen so an, dass nur Freunde die geposteten Inhalte sehen können. Sind die Inhalte für alle sichtbar, sind diese auch für Mobber einsehbar und können von ihnen für ihre Attacken missbraucht werden.
- Verbirg deine Kontaktdaten: Entscheide dich von Fall zu Fall, wer von deinen Freunden deine Handynummer, Anschrift oder E-Mail-Adressen sehen oder erhalten soll. Sind die Kontaktdaten für alle einsehbar, können sie in falsche Hände geraten.
- Fordere das „Recht auf Bildnis“ ein: Werden auf Partys Fotos geknipst, frag den Fotografen, was er mit den Fotos machen will und

Stop IT

Stop-IT (http://www.stop-it.org/) ist Mitglied von INHOBE (http://www.inhope.org/gns/home.aspx), das ist eine Vereinigung internationaler Meldestellen für illegale Inhalte im Netz, wie Anstiftung zur Gewalt, Rechtsradikalismus oder Pädophilie.

Post- und Kommunikationspolizei

Reschenstraße 190
39100 Bozen
E-Mail: sez.polposta.bz@pecps.poliziadistato
Tel.: 0471/531411/19/16/13 oder 0471/531512

ersuche ihn eindrücklich, die Fotos nicht in soziale Netzwerke zu stellen.

- Prüfe Freundschaftsanfragen: Hinter einer unscheinbaren Kontaktanfrage kann sich auch ein Mobber verbergen. Erkundige dich nach der Vertrauenswürdigkeit der Anfrage, bevor du die Kontaktanfrage fremder Personen bestätigst. Blockiere in jedem Fall vorerst den Zugriff unbekannter Personen auf deine privaten Fotos und privaten Infos.

Gegenmaßnahmen

Ist der Ernstfall eingetreten, dann wähle am besten eine abgestufte Reaktion je nach Schwere des Angriffs. Reagiere nicht reflexartig und mit Wut im Bauch, sondern schlafe eine Nacht darüber.

Facebook Europa

Facebook Ireland Limited Hanover Reach
5-7 Hanover Quay
Dublin 2
Ireland
http://www.facebook.com/legal/terms?locale=de_DE

- Sichere Beweise: Mobbing-Inhalte solltest du zur Beweissicherung speichern. Mache einen Screenshot („Bildschirmfoto“) von Texten und Fotos, lade die Videos auf deine Festplatte herunter und notiere dir Datum und Uhrzeit der Mobbing-Vorfälle. Am besten ist, wenn auch Zeugen die Vorfälle bestätigen können.
- Stelle den Mobber zur Rede: Kennst du den Mobber, dann solltest du ihm klar machen, dass so was nicht geht. Ein solches Gespräch sollte nur im Beisein von Zeugen geführt werden. Als Zeuge kann im Schulumfeld der Vertrauenslehrer, der Direktor oder der Mediator auftreten.
- Blockiere den Kontakt: Ist der Mobber ein Freund auf Facebook, kannst du ihn aus deiner Freundesliste entfernen, die beleidigenden Beiträge aus deiner Chronik löschen. So kann der Mobber nicht mehr auf deine Chronik schreiben. Ändere deine Handynummer oder E-Mail-Adresse, sodass der Mobber dich nicht mehr mit seinen Angriffen erreichen kann.
- Schalte den Anwalt oder die Polizei ein: In gravierenden Fällen kannst du nach einer Rechtsberatung den Mobbing-Vorfall zur Anzeige bringen. Der Betreiber des sozialen Netzwerkes kann dann aufgefordert werden, die rechtswidrigen Inhalte umgehend zu löschen.[142]

142 Facebook-Link für Anwälte und Polizei: http://www.facebook.com/safety/groups/law/guidelines

3.7 Problemfälle und Alternativen

Facebook ist ein soziales Netzwerk im permanenten Wandel. Ständig kommen neue Funktionen hinzu und Nutzungsbedingungen können schon mal über Nacht geändert werden. Nicht immer erschließt sich, wo sich die Stellschrauben für die Anpassungen der Privatsphäre-Einstellungen befinden. Die Privatsphäre-Modi sollten nutzerfreundlicher angepasst werden können. Klare Mängel weist Facebook beim Datenschutz auf und stellt in jedem Fall ein Problem für den Datenschutz im europäischen Verständnis dar (Artt. 11, 13, 23, 24 D.lgs. 196/2003).

Problemfall Opt-out-Prinzip

Auf Facebook gilt das sogenannte Opt-out-Prinzip. Mark Zuckerberg, Gründer von Facebook, stellte fest, dass die Privatheit nicht mehr zeitgemäß und dass Offenheit die neue „soziale Norm" sei. Die Opt-out-Regel ist ein klarer Verstoß gegen den italienischen Datenschutzkodex, dem das Opt-in-Prinzip zugrunde liegt. Danach muss nämlich der Nutzer aktiv werden, um private Daten freizuschalten. Zudem muss der Betroffene eine bewusste und informierte Einwilligung abgeben, bevor Personendaten gesammelt und verarbeitet werden können. Der Einwilligung muss in allgemein verständlicher Form eine Datenschutzbelehrung vorangehen, die über Zweck, Verarbeitung oder Weitergabe der Personendaten aufklärt.

Problemfall „Gefällt-mir"-Button

Facebook ist auch außerhalb der virtuellen Grenzen der Plattform präsent. Surfer stoßen überall im Netz auf das kleine weiße „f" vor blauem Hintergrund, dem sogenannten „Gefällt-mir"-Button. Facebook-Nutzer, die darauf klicken, bekunden, dass ihnen ein bestimmter Online-Inhalt, wie ein Zeitungsartikel, ein Produkt oder Foto gefällt. Klickst du auf den „Gefällt-mir"-Button, dann erscheint in der Facebook-Timeline ein Status-Update, dass „(>Facebook-Name<) der Film (>Titel<)" gefällt und im Abschnitt *Gefällt mir & Interessen* der Profilseite kommt der „gelikte" Online-Inhalt hinzu. Deine Facebook-Kontakte werden dann via News Feed automatisch über deine neuen Vorlieben informiert. Mit dem Klick auf das *„f"*, wirst du ungewollt zum Werbeträger. Für die Betreiber der Webseiten ist der „Gefällt-mir"-Button ein wirksames Instrument, für Aufmerksamkeit und weitere Verbreitung der eigenen Inhalte zu sorgen. Die Werbewirtschaft geht davon aus, dass Webseiten, die von deinen Freunden „gelikt" wurden, demnächst auch von dir aufgerufen und als gut befunden und so via Schneeballsystem immer bekannter werden. Schließlich geben die „Gefällt-mir"-Buttons

Tipp

Willst du nicht, dass dich Facebook oder auch andere soziale Plattformen auf „Schritt und Klick" im Internet tracken, dann logge dich aus, bevor du im Netz surfst. Die abgelegten Cookies kannst du mit Reinigungstools wie CCleaner entfernen.

Auskunft darüber, wer du bist. Forscher der University of Cambridge können ausschließlich auf der Grundlage der angeklickten Likes mit einer Trefferquote von bis zu 95 Prozent ermitteln, ob der Nutzer etwa „Raucher, konservativ oder schwul“[143] ist.

Abb. 20: Datenschutzkonformer Gefällt-mir-Button

Datenschutzrechtlich ist der „Gefällt-mir“-Button ein Problem. Rufst du eine Webseite auf, in welcher der „Gefällt-mir“-Button eingebettet ist, dann wird der Button nicht vom Server der aufgerufenen Webseite, sondern direkt vom Facebook-Server in den Browser nachgeladen. Nun muss Facebook noch den Surfer identifizieren, der den „Like“-Button angeklickt hat. Dazu sucht ein Skript nach Cookies auf deinem PC, die Facebook bei jedem deiner Besuche dort hinterlegt hat. Ohne dein Wissen und ohne dein Okay erhält Facebook so Informationen darüber, was dich im Netz interessiert und welche Vorlieben du hast.

Der Computerverlag Heise[144] hat eine datenschutzkonforme 2-Klick-Lösung entworfen. Danach werden standardmäßig keine Surfdaten an die Betreiber der sozialen Netzwerke übertragen. In der Voreinstellung sind die Buttons deaktiviert (ausgegraut). Erst wenn der Surfer den ausgegrauten Button anklickt, wird dieser aktiviert. Der erste Klick bedeutet zudem, dass der Surfer seine Einwilligung dazu erteilt, dass Daten an die jeweiligen Betreiber der sozialen Netzwerke gesendet werden. Mit dem zweiten Klick kann der Nutzer seine gewohnte Empfehlung übermitteln. Die Buttons lassen sich auch dauerhaft aktivieren. Dazu muss man nur unter dem Zahnrad-Icon das passende Häkchen setzen.

Facebook-Account löschen

Willst du Facebook den Rücken kehren, solltest du zuvor dein Konto aufräumen und alle Datenspuren löschen. Die Löschfunktion ist bei Facebook gut versteckt. Klicke oben rechts auf den kleinen Pfeil und wähle anschließend *Hilfe*. Über den Link *Besuche den Hilfebereich* unten links gelangst du auf eine Übersichtsseite. Dort wählst du links *Verwalte dein Konto* und klickst auf *Konten deaktivieren, löschen und in den Gedenkzustand versetzten*. Unter der Überschrift *Konten löschen* klicke nun auf *Wie lösche ich mein Konto dauerhaft?* und am Ende des ersten Absatzes auf den Link: *teile es uns mit*. Im nächsten Dialogfenster startest du mit dem Klick auf *Mein Konto löschen* den Löschvorgang.

143 Holger Dambeck (2013): *Zeig mir deine Likes - und ich weiß, wer du bist,* Spiegel online, 11. März 2013, 21:06 Uhr, URL: http://www.spiegel.de/netzwelt/web/facebook-studie-likes-enthuellen-persoenlichkeit-a-888151.html. Forscher des amerikanischen IT-Konzerns IBM haben herausgefunden, dass ihnen bereits 50 Tweets reichen, um die Persönlichkeit eines Menschen als „ziemlich gut“ und 200 Tweets um sie als „sehr gut“ bestimmen zu können. Die Persönlichkeitsmerkmale interessieren die Werbeindustrie. Wissen die Vermarkter wer der Surfer ist, können sie zielgenau Werbung einspielen: http://www.zeit.de/digital/internet/2013-06/twitter-psychologie-persoenlichkeit

144 http://www.heise.de/extras/socialshareprivacy/

Problemfall Datenverbindungen

Mit etwas Selbstdisziplin können Facebook-Nutzer ihre Privatsphäre durch Datensparsamkeit schützen. Nutzer müssen nicht ins Profil hineinschreiben, dass sie beispielsweise überzeugte Anhänger der Lichtnahrung sind. Verzichten sie auch darauf, entsprechende Kommentare auf Facebook einzustellen, sollten ihre innersten Überzeugungen eigentlich geheim bleiben. Neue Analysetechniken ermöglichen jedoch, Überzeugungen oder Interessen freizulegen, die letztlich privat bleiben sollten. Wer eine Freundesliste mit Lichtessern unterhält, die sich in ihren Profilen und Chroniken als solche outen, findet mit einer gewissen Wahrscheinlichkeit selbst Gefallen an der Idee der Lichtnahrung. Die zugrunde liegende Annahme der Analysten lautet: „Zeig mir deine Freunde, und ich sag dir, wer du bist.“ Der springende Punkt bei solchen Datenverknüpfungen ist, dass die Nutzer nicht wissen, mit welchen anderen Datenbeständen ihre Daten verknüpft werden und für welche Zwecke die so gewonnenen Erkenntnisse verwendet werden. Kann aus der Freundesliste abgelesen werden, an welche esoterische Methode Nutzer glauben oder welche politische Ein-

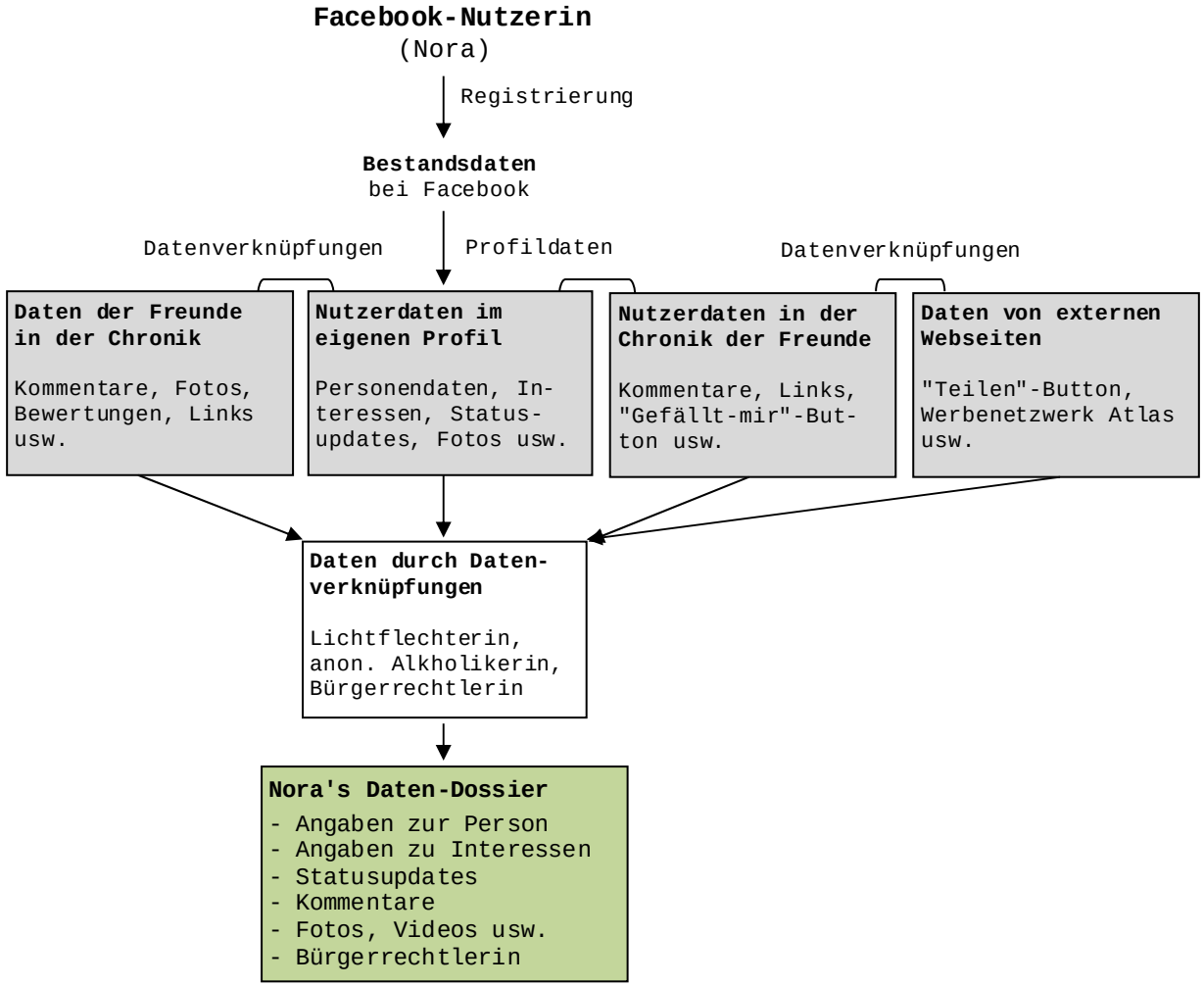


Abb. 21: Web 2.0-Datenflut und Datenverbindungen

stellung sie haben, dann hat der Nutzer nicht mehr die Kontrolle über die Frage, was er privat halten und was er publik machen möchte. Haben Nutzer, die in einer Wohngegend mit niedrigem Einkommensniveau, hoher Arbeitslosigkeit und schlechter Zahlungsmoral wohnen, schlechtere Karten bei der Gewährung eines Verbraucherkredites und müssen sie mit einem entsprechenden Risikoaufschlag rechnen, dann sind solche soziale Umfeldanalysen mit handfesten wirtschaftlichen Nachteilen verbunden.

Problemfall Datenflut

Die Facebook-Dienste sind nur auf den ersten Blick kostenlos. Der Betrieb von Facebook wird hauptsächlich über personalisierte Werbung finanziert. Zielgenaue Werbung ist allerdings nur möglich, wenn Werbeagenturen so viel wie möglich von dem wissen, was Nutzer im sozialen Netzwerk an Personendaten preisgeben, was sie an Inhalten auf Facebook posten und was sie auf externen Webseiten interessiert. Die so erzeugte Datenflut kollidiert mit dem Grundsatz der Datenvermeidung.

Problemfall Facebook-„Filter-Bubble“

Der Autor Eli Pariser hat mit dem Begriff „Filter-Bubble“ auf die Gefahr hingewiesen, dass mit dem Zugang zu Informationen über soziale Netzwerke, Nutzer nur jene Informationen erhalten, die zum eigenen Profil passen. Der Nutzer wählt die Filter nicht selbst, sondern sie werden von gewinnorientierten Unternehmen eingesetzt. Die Gemeinschaften, die über Facebook entstehen, erzeugen so homogene Welten, in denen Freunde, die weitgehend dieselben Interessen und Auffassungen haben, Freunde „liken“. Findet kein Austausch kontroverser Meinungen statt, können Menschen auch nicht umdenken und dazulernen. Gehen aber der Wille und die Bereitschaft verloren, die Argumente Andersdenkender anzuhören und zu prüfen, dann könnte die „Filter-Bubble“ in Zukunft die Bildung einer politischen Öffentlichkeit erschweren, die das Wohl der ganzen Gesellschaft im Blick hat.

Alternativen zu Facebook

Facebook ist mit mehr als einer Milliarde Nutzer das marktbeherrschende soziale Netzwerk. Es gibt aber eine Reihe von Alternativen zu Facebook, welche die Kontrolle über die Privatsphäre anders regeln, eine andere Zielgruppe im Blick haben und ein eigenes Geschäftsmodell unterhalten. Der Markt der sozialen Netzwerke ist von einem Prozess „schöpferischer Zerstörung“[145] charakterisiert. Neue Ideen und Konzepte können etablierte Anbieter in wenigen Jahren in Bedrängnis bringen. Ob Facebook in zehn Jahren auch noch den Inbegriff für ein soziales Netzwerk darstellt, kann niemand vorhersagen.

Netzwerke	Webadresse	Kurzbeschreibung
Google+	https://plus.google.com	Goole+ ist ein soziales Netzwerk der Firma Google Inc. Google+ führt die verschiedenen Google-Dienste, wie Gmail, YouTube, Google-Websuche oder Google-Docs zusammen und kann so die Daten aus allen Diensten zu einem Superprofil verknüpfen. Finanziert wird der kostenlose Dienst über Werbeeinnahmen.
Flickr	www.flickr.com	Flickr ist vorrangig ein Online-Fotoportal der Firma Yahoo. Jeder kann kostenlos Fotos ansehen, registrierte Nutzer können Fotos speichern und kommentieren. Fotos können auch unter der Creative Commons-Lizenz veröffentlich werden, die dem Nutzer erlaubt, die Fotos beispielsweise für nichtkommerzielle Zwecke zu nutzen und weiterzuverarbeiten.
Friendica	http://friendica.com	Friendica ist ein Open-Source-Netzwerk, das sich noch im Entwicklungsstadium befindet. Im Mittelpunkt steht der Schutz der Privacy. Anders als Facebook oder Google+ ist friendica ein dezentrales, ein Peer-to-Peer-Netzwerk.
Pinterest	http://pinterest.com	Pinterest ist ein kostenloser Dienst der Firma Cold Brew Labs, Inc. Nutzer können Fotos/Videos einstellen und an die Pinnwand „anheften“ und sich darüber mit anderen Nutzern austauschen.
Twitter	https://twitter.com	Twitter ist ein Microblogging-Dienst der Firma Twitter Inc. Nutzer können kostenlos Kurznachrichten von maximal 140 Zeichen posten. Im Gegenzug sammelt Twitter personenbezogenen Daten, um sie zu vermarkten. Wie Twitter langfristig die Finanzierung der Infrastruktur sichert, ist derzeit noch unklar.

145 Den Begriff „schöpferische Zerstörung“ hat der Ökonom Joseph Alois Schumpeter (1883-1950) geprägt. Für Schumpeter bestand der Wettbewerb auf Märkten insbesondere darin, dass neue Waren und Produktionsverfahren alte Waren und Produktionsverfahren verdrängen. Eine Schlüsselrolle nehmen hierbei die Pionierunternehmer ein.

Netzwerke	Webadresse	Kurzbeschreibung
YouTube	http://www.youtube.com	YouTube ist ein kostenloses Online-Videoportal der Firma Google Inc. Jeder kann Videos ansehen, registrierte Nutzer können Videos hochladen und bewerten. Finanziert wird der Dienst durch Werbeeinnahmen.
XING	www.xing.com	XING ist ein Netzwerk der Firma Xing AG für Geschäftskontakte und Jobsuche; berufliche Profilinformationen bilden die Grundlage für die Netzaktivitäten. Es handelt sich um ein Freemium-Modell: das Basisangebot ist gratis, das Premium-Angebot ist kostenpflichtig. Finanziert wird die Plattform zudem durch Werbeeinnahmen.

Tab. 11: Alternativen zu Facebook

3.8 Arbeitsaufträge

1. Wie kannst du auf Facebook überprüfen, was ein Fremder von deinem Profil im Einzelnen sieht?

2. Welche Voreinstellungen musst du ändern, dass in Facebook einzelne Informationen nur eine bestimmte Person sehen kann?

3. Wie kannst du deine Fotos in Facebook vor den neugierigen Blicken von Fremden schützen?

4. Überlege, warum es datenschutzrechtlich problematisch ist, Facebook Zugriff auf dein E-Mail-Konto zu gewähren. Liste auf, welche Informationen Facebook mit dem Zugriff erhalten kann und für welche Zwecke Facebook diese Informationen verwenden könnte.

5. Darfst du so ohne Weiteres Comic-Helden wie Donald Duck oder Asterix als Profilbild für dein Facebook-Konto verwenden?

6. Welche Medieninhalte darfst du bei Facebook ungefragt veröffentlichen?

7. Wann liegt eine „Veröffentlichung“ von Inhalten bei Facebook vor? Liegt eine Veröffentlichung vor, wenn „nur ich“, „Benutzerdefiniert“, „Freunde“, „Freunde von Freunden“ oder alle den Inhalt sehen können?

8. Darfst du so ohne Weiteres ein YouTube-Video in die eigene Facebook-Seite einbinden?

9. Gilt das Zitatrecht auch in der Facebook-Chronik? Darf man hier nach Belieben urheberrechtlich geschützte Texte, Fotos oder Videoclips verlinken?

10. Welche Rechte erwirbt Facebook für Fotos und Videos, die Nutzer bei Facebook einstellen?[146]

11. Der Architekt vereinbart mit der Fotografin, dass er die ausschließlichen Nutzungsrechte an den gemachten Architekturfotos hat, sie diese aber für Eigenwerbung nutzen darf. Monate später beschließt die Fotografin, einige dieser Fotos bei Facebook einzustellen, um auf sich als Architekturfotografin aufmerksam zu machen. Darf sie das?

146 Jeder, der sich bei Facebook registriert, muss zuvor dessen Nutzungsbedingungen anerkennen. Vgl. Ziffer 2.1: https://de-de.facebook.com/legal/terms?locale=de_DE

a) Hat die Fotografin die entsprechenden Bildrechte im Verhältnis zum Architekten?
b) Hat die Fotografin die entsprechenden Bildrechte im Verhältnis zu Facebook?[147]

12. Welche Bildrechte räumen Nutzer der Fotoplattform Flickr ein, wenn sie Bilder auf die Plattform hochladen?[148]

13. Haftet der Inhaber einer Profilseite bei Facebook auch für die Kommentare und Fotos, die andere bei ihm posten?

14. Erstellt zu dritt eine Liste an Online-Inhalten, die in Facebook nicht veröffentlicht werden dürfen. Stellt die Ergebnisse der Klasse vor.

a) Welche Online-Inhalte sind rechtswidrig? Führt hierzu auch die entsprechenden Strafrechtsnormen an.
b) Welche Online-Inhalte sind nach der Hausordnung von Facebook verboten?
c) Welche Online-Inhalte sind rechtlich nicht verboten, aber für Kinder und Jugendliche nicht geeignet?

15. Wie kann man in Facebook Nazis, Faschisten und andere Extremisten erkennen? Was kann man tun, wenn man in Facebook auf verfassungswidrige Inhalte stößt?

16. Bearbeitet in Gruppen die Problematik des sogenannten Cybermobbings.

Gruppe A beschäftigt sich mit der Frage, was Mobbing und speziell Cybermobbing ist.

a) Welche Erscheinungsformen des Cybermobbings gibt es? Recherchiert nach Fotos und Videos, die klar als Mobbing gewertet werden können.
b) Was bewirkt Mobbing bei den Betroffenen?

Gruppe B geht der Frage nach, welche Strafen dem Mobber bzw. der Mobberin drohen.

a) Welche Handlungen sind strafrechtlich verboten?
b) Wie bringt man Mobbing zur Anzeige: Gibt es hierzu Vordrucke? Wo macht man die Anzeige? Wer ist befugt, Anzeige zu erstatten?

147 Bildrechte bei Facebook: „Du wirst keine Inhalte auf Facebook posten oder Handlungen auf Facebook durchführen, welche die Rechte einer anderen Person verletzen oder auf sonstige Art gegen das Gesetz verstoßen“ (Ziffer 5.1): https://de-de.facebook.com/legal/terms?locale=de_DE. Diese Facebook-Klausel besagt, dass nur Fotos eingestellt werden dürfen, die frei von Rechten Dritter sind.

148 Bildrechte bei Flickr: https://policies.yahoo.com/ie/de/yahoo/terms/utos/index.htm; https://blog.flickr.net/de/2011/05/23/auf-flickr-gehoren-eure-fotos-euch/

Gruppe C befasst sich mit der Frage, wie man Mobbing vorbeugen kann.

a) Was kannst du als Einzelner tun, um nicht Mobbing-Opfer in sozialen Netzwerken zu werden? Erstellt hierzu ein Plakat.
b) Was tut eure Schule, um Mobbing zu ächten?
c) Wie sollte Mobbing in der Schulordnung geahndet werden?

17. Die Klasse sieht sich die DVD „Homevideo“ von Kilian Riedhof an und bearbeitet in Gruppen folgende Fragestellungen:

a) Wie haben sich die Eltern von Jakob verhalten? Wie hätten sie Jakob helfen können?
b) Wie haben sich die Mitschüler im Film verhalten? Was können Mitschüler tun, um Mobbing zu verhindern?
c) Wie haben sich die Lehrer und die Schulleitung verhalten? Was hätten sie anders machen sollen?
d) Wie hätte sich Jakob selbst vor Mobbing besser schützen können?

18. Untersucht, wie die Freundschaft zwischen Mädchen in den 1960er Jahren und wie sie heute in den sozialen Netzwerken gepflegt wird. Bildet für die Analyse zwei Gruppen und stellt die Ergebnisse der Klasse vor.

Gruppe A befasst sich mit dem Kinderfilm „Pippi geht von Bord“ von Astrid Lindgren aus dem Jahr 1969.

a) Sammelt Äußerungen von Pippi, bei denen es um Freundschaftsbekundungen geht.
b) Zu welcher Uhrzeit ist im Film Zeit für die Freundschaftspflege?
c) …

Gruppe B beschäftigt sich mit der Sprache von Mädchenfreundschaften auf Facebook.

a) Untersucht die Sprache ihrer Postings.
b) Wie oft wird täglich/wöchentlich gepostet?
c) Innerhalb welcher Zeit reagieren Freundinnen mit einem Kommentar?
d) Wer kann der Freundschaftsinszenierung zusehen?

19. Einzelne Personendaten, die beim Surfen gesammelt werden, können unproblematisch sein; werden die Daten miteinander verknüpft, kann ein detailreiches Bild über eine Person entstehen. Macht als Übung eine Online-Ermittlung zu zwei Mitschülern aus eurer Klasse - natürlich mit ihrer ausdrücklichen Zustimmung - und stellt auch die Ermittlungsergebnisse nur mit ihrer Zustimmung der Klasse vor.

a) Sucht über die Websuche sowie Personensuchmaschinen nach den Mitschülern und protokolliert die Suchergebnisse.

b) Recherchiert über den Dienst NameChk,[149] in welchen Netzwerken die Schüler präsent sind.
c) Ermittelt, welche Informationen in den Profilen der sozialen Netzwerke für „alle“ sichtbar sind.
d) Findet heraus, welche Informationen die Freunde der beiden Mitschüler über diese gepostet haben.
e) Ladet alle Fotos aus den sozialen Netzwerken herunter, auf denen die Mitschüler zu sehen sind.
f) Erstellt nun mithilfe der gesammelten Informationen ein Dossier von euren Mitschülern, das für die Werbeindustrie relevant sein könnte.

20. Recherchiere nach deinem Ruf im Netz.

a) Gib deinen Vor- und Nachnamen bei Google ein und notiere dir, welche Informationen über dich im Netz zu finden sind.
b) Schlüpfe nun in die Rolle des Chefs einer kleinen Firma, bei der du dich für das Sommerpraktikum beworben hast. Würdest du dir aufgrund deines Netzrufes den Sommerjob geben?

21. Facebook wird auch von Freiberuflern und Kleinbetrieben geschäftlich genutzt. Betreibt ihr an eurer Schule eine Übungsfirma (ÜFA), dann richtet für sie eine Firmenseite bei Facebook ein.

Gruppe A beschäftigt sich mit der Einrichtung einer Fanpage.

a) Welches Icon sollte die Firma repräsentieren?
b) Erstellt Fotos für die Bildergalerien und erklärt, warum diese für Facebook geeignet sind.
c) Besteht für die Fanpage eine Impressumspflicht?
d) Stellt Informationen über die Firma zusammen, welche die Besucher der Fanpage interessieren könnten.

Gruppe B beschäftigt sich mit der Pflege des Webauftritts.

a) Wer von der Firma ist der Facebook-Beauftragte?
b) Wie viel Zeit ist für die Pflege der Fanpage eingeplant: wöchentlich, täglich?
c) Rechnet sich für die Firma der Zeitaufwand für die Pflege der Fanpage?
d) Welche Informationen und Medieninhalte sollten gepostet werden? Darf auch Privates von Mitarbeitern der Firma veröffentlicht werden?
e) Was versteht die Firma unter der arbeitsrechtlichen Treuepflicht des Facebook-Beauftragten?

Gruppe C beschäftigt sich mit der Social-Media-Kompetenz der Firma.

a) Dürfen die Fans auch auf die Chronik posten? Klärt, warum ihr die Interaktion mit den Fans ermöglichen oder unterbinden wollt.
b) Erstellt einen Plan, wie ihr schnell zu einem „Grundstock“ an Fans kommt.

149 http://namechk.com/

c) In welchem Verhältnis soll Werbung zu Informationen über Produkte, Tipps oder Support stehen?
d) Welche Links zu interessanten Artikeln und Videoclips passen zu eurem Webauftritt?
e) Wie sollten die treuen Kunden bei der Stange gehalten werden? Wie sollten neue Kunden gewonnen werden?
f) Wie sollte der Facebook-Beauftragte mit Kritik der Fans zu Produkten, Service oder Gewährleistung umgehen?

22. Facebook kann auch für politische Ziele genutzt werden.

a) Sucht in Facebook nach Politikerinnen und Politikern, die das soziale Netzwerk dazu nutzen, politische Vorhaben mit den Bürgern zu diskutieren.
b) Recherchiert in Facebook nach lokalen politischen Initiativen, die von Bürgerinnen und Bürgern ausgehen.
c) Überlegt, wie autoritäre Staaten mithilfe von Facebook politische Gegner identifizieren können.

23. Wer eigene anzügliche Partyfotos in soziale Netzwerke stellt, disqualifiziert sich für Bewerbungsgespräche, ist vielfach zu lesen.

a) Besteht ein nachweisbarer Zusammenhang zwischen den Freizeitaktivitäten der Arbeitssuchenden und ihrer professionellen Eignung?
b) Hat der Arbeitgeber ein berechtigtes Interesse, seine Vorstellungen aus der Arbeitswelt auf die private Lebenswelt der Arbeitssuchenden ausdehnen?
c) Macht Vorschläge, wie in den sozialen Medien die Grenzlinie zwischen Privatem und Arbeitswelt neu gezogen werden sollte.

24. Vergleicht, welche Risiken beim Telefonieren und welche beim Austausch von Informationen über soziale Netzwerke bestehen.

a) Wie lässt sich die Identität beim Telefonieren feststellen? Wie lässt sich im Internet klären, wer Absender und Empfänger von Informationen ist?
b) Wie kann man Vertraulichkeit beim Telefonieren sicherstellen? Wie kann man die Vertraulichkeit bei einer Internetkommunikation sicherstellen?

25. Informationelle Selbstbestimmung heißt, dass du bestimmst, wer von dir Personendaten erheben und verwenden darf. Versuche eine Liste zu erstellen, wer welche Personendaten von dir kennt: deine Rufnummer, deine E-Mail-Adresse, deine Chat-Adresse, dein Profil in Facebook & Co und deine Anschrift.

4 Smartphone sicher nutzen

Leitfragen

- Was sollst du beim Abschluss eines Handyvertrages beachten?
- Wann darf die Polizei Telefonate der Bürger mitschneiden?
- Dürfen Geheimdienste Bürger fremder Staaten anlasslos überwachen?
- Wie kannst du ermitteln, welche Daten Apps ohne deine Einwilligung abfragen?
- Wie kannst du deine Telefonate, E-Mails oder Chats vor Datenspionen und Lauschern schützen?
- Wie kannst du deine vertraulichen Daten auf dem Smartphone vor Angriffen schützen?

Für Schüler und Jugendliche sind heute PC, Internet und Smartphone dank Flatrate Alltag. Insbesondere das Smartphone nimmt unter den Neuen Medien eine herausragende Stellung ein. Smartphones lassen sich nutzen als Mobiltelefon, Terminkalender, Webbrowser, Mediaplayer, Radio, Foto- und Videobetrachter sowie Foto- und Videokamera, GPS-Navigationsgerät, Spielekonsole, Diktiergerät oder Datenspeicher und zum Versenden von E-Mails und SMS. Das Smartphone ist zu einer wichtigen Datenzentrale für sensible Daten geworden. Verbindet man all diese Daten miteinander, geben sie Auskunft darüber, wer der Nutzer ist.

Wer Smartphones nutzt, setzt sich Risiken aus. Telefongespräche können abgehört, SMS abgefangen, vertrauliche Daten ausspioniert und das Surfverhalten kann getrackt werden. Die so gewonnenen Daten können für personalisierte Werbung oder auch für illegale Geschäfte verwendet werden, etwa dem Kauf von Waren bei eBay unter falschem Namen.

Vor den Risiken können sich die Nutzer durch Recht und Technik schützen. Das moderne Datenschutzrecht wurde entwickelt, um dem Nutzer auch im digitalisierten Umfeld ein Recht auf „informationelle Selbstbestimmung“ zu gewährleisten. Dieses Recht besagt, dass jeder Nutzer autonom entscheiden kann, ob und welche Personendaten er preisgeben will und wie sie verwendet werden dürfen. Ein wirksamer Schutz der Privatsphäre erfordert Recht und Technik. Der Nutzer muss fähig sein, selbst für den Schutz seiner Daten sorgen zu können. Insbesondere muss er wissen, wie man Vertraulichkeit, Unversehrtheit, Authentizität und

Verfügbarkeit der Daten wahren kann. Dieses Kapitel zeigt auf, wie du deine digitale Privatsphäre[150] selbst schützen kannst; also, was du tun kannst, damit dein Surfverhalten nicht getrackt wird, dass du vertraulich kommunizieren oder „gute“ von „schlechten“ Apps unterscheiden kannst.

Wie wirst du zum autonomen und kritischen Smartphone-Nutzer? Indem du selbst kleine Sicherheitsschritte wagst, etwa selbst ein Antivirenprogramm auf dem Smartphone installierst oder Apps erst dann ausprobierst, nachdem du im Internet über ihre Verlässlichkeit recherchiert hast. Am Ende wächst die Urteilskompetenz, wie du deine digitale Privatsphäre wirksam schützen kannst.

Was bedeutet Privatsphäre?

- Die „lokale Privatsphäre“ ist ein Ort, wo Personen ohne Maske leben können. Der Inhaber eine Wohnung kann bestimmen, wer sie betritt, wie sie gestaltet ist und welche Regeln dort gelten. Die „Unverletzlichkeit der Wohnung“ gehört zu den klassischen Grundrechten (Art. 14 Verf.).
- Bei der „sozialen Privatsphäre“ treten Personen in Beziehung mit anderen, etwa indem sie sich bei vertrauten Personen etwas „von der Seele reden“, sich in der Öffentlichkeit mit ihrem ausgefallenen Haarschnitt zeigen, ohne dass andere darüber lästern.
- Die „digitale Privatsphäre“ bezieht sich darauf, dass Personen selbst über die Weitergabe und Verwendung von personenbezogenen Daten bestimmen dürfen. Ihr Schutz setzt Recht, Technik und Medienkompetenz voraus.

4.1 Abschluss eines Handyvertrages

Schließen wir erst mal einen Handyvertrag ab. Der Handyvertrag kommt durch „Einigung“ zwischen dir und dem Mobilfunkanbieter zustande. Auf Vertragsangebote übers Telefon solltest du nicht eingehen, du könntest vorschnelle Entscheidungen treffen. Lass dir am besten die Internetadresse der Webseite geben, auf der du in aller Ruhe das Angebot prüfen kannst. Gib auch vorerst keine Auskunft über Personendaten und Anschrift, sondern gib diese Daten erst dann weiter, nachdem dich das Angebot überzeugt hat. Der Handyvertrag kann auch per E-Mail oder per Mausklick auf den Ja-Button auf der Webseite des Mobilfunkanbieters abgeschlossen werden. Schließt du den Handyvertrag online ab, hast du eine Widerrufsfrist von zehn Werktagen. Willst du den Handyvertrag widerrufen, musst du die Widerrufserklärung unterzeichnen und per „Einschreiben mit Empfangsbestätigung“ an den Mobilfunkanbieter richten.

Lies mit Sorgfalt die Datenschutzbelehrung des Mobilfunkanbieters durch und prüfe, ob die Personendaten für Werbung verwendet werden, ob die Rufnummer an Dritte weitergegeben wird und ob Werbeanrufe erlaubt sind oder nicht. Willst du von lästigen Werbeanrufen verschont bleiben, dann deaktiviere die entsprechenden Kontrollkästchen. Am besten ist, du lädst dir den Vertragsinhalt von der Webseite herunter, druckst

150 Überblick über die Formen der Privatsphäre: Sabine Trepte (2012): *Privatsphäre aus psychologischer Sicht,* in: Jan-Hinrik Schmidt u. a. (Hrsg.): *Datenschutz,* Bonn 2012, S. 59-66; zur Diskussion um die digitale Privatsphäre: APuZ 15-16/2013: *Transparenz und Privatsphäre,* http://www.bpb.de/shop/zeitschriften/apuz/157554/transparenz-und-privatsphaere; zum Ende der Privatsphäre: Christian Heller (2011): *POST-PRIVACY. Prima leben ohne Privatsphäre,* München.

ihn aus, unterschreibst ihn und sendest ihn per Post an den Mobilfunkanbieter. Hast du den Online-Abschluss gewählt, dann sichere dir zum Nachweis den Vertragsinhalt per Screenshot oder lade ihn dir, falls vorgesehen, als PDF-Datei auf deinen PC herunter.

Willst du sparen, musst du dich über die Handytarife informieren. Das ist wegen des Tarifdschungels schwierig. Der auf den ersten Blick günstige Tarif kann in der Endabrechnung schnell teuer werden, weil das gewählte Datenpaket nicht zu deinem tatsächlichen Nutzerverhalten passt.

Tipps für den Handyvertrag

- Wie nutzt du dein Handy? Nur zum Telefonieren, auch für SMS, E-Mail-Abfragen oder auch für Internetradios, Podcasts oder Internetvideos? In welchem Umfang nutzt du die einzelnen Dienste am Tag, im Monat?
- Welche Netze nutzen deine Freunde? Bedenke, deine Freunde sind auch deine häufigsten Gesprächspartner. Wähle den Netzbetreiber deiner Freunde, denn netzinterne Gespräche sind in der Regel günstiger als netzexterne. Ein Kriterium der Netzwahl kann auch die Netzabdeckung sein, insbesondere in Randgebieten oder auf dem Land.
- Welches Internetpaket passt zu deinem Nutzerverhalten? Jeder Klick auf eine Webseite, jeder Aufruf eines Fotos oder eines Videos verursacht einen Datenverkehr zwischen Provider und Browser. Surfst du nur gelegentlich im Netz und rufst nur Mails mit Textnachrichten ab und siehst du dir nur ab und zu bei YouTube Kurzvideos an, dann reicht ein Datenvolumen von etwa 500 MB. Nutzt du täglich Internetradios, Podcasts oder lädst Software aus dem Netz, solltest du ein größeres Datenpaket mit mehreren Gigabyte Volumen in Betracht ziehen.
- Verschaffe dir einen Überblick über die Handytarife. Informiere dich im Vorfeld genau über die Handytarife – etwa monatliche Fixkosten, Kosten für Telefonate, SMS, Internetpaket, Laufzeit. Handytarife vergleichen kannst du beispielsweise auf der Homepage der Verbraucherzentrale Südtirol unter dem Link „Tarifwegweiser für Festnetz und Handy“ (www.verbraucherzentrale.it) oder auch unter: www.tariffe.it

4.2 Grundrecht auf vertrauliche Telekommunikation

4.2.1 Überwachung durch Polizei

4.2.1.1 Wann darf überwacht werden?

Die Telekommunikation steht unter dem besonderen Schutz der Verfassung und ist ein Menschenrecht.[151] Telefonate, E-Mail-Nachrichten oder Chats dürfen nicht so ohne Weiteres von Strafverfolgungsbehörden überwacht werden. Die vertrauliche Kommunikation ist ein unverletzliches Grundrecht, das dem Bürger Freiräume einräumt, in die der Staat grundsätzlich nicht eingreifen darf. Die italienische Verfassung schützt ausdrücklich das Briefgeheimnis und „jede andere Form der Mitteilung“ (Art. 15 I Verf.). Unter „jede andere Form der Mitteilung“ fällt heute auch die Telekommunikation, also die Kommunikation über Kabel, Mobilfunk oder Satellitenfunksysteme. Du hast also ein Grundrecht darauf, lauschfrei zu telefonieren und Informationen per SMS, E-Mail oder Chat unbeobachtet vom Staat auszutauschen. Der Schutz der Telekommunikation umfasst auch die Frage mit wem, wann, wo und wie lange du kommuniziert hast.

151 In der Resolution vom 18.12.2013 fordert die UN-Generalversammlung „alle Staaten“ auf, das „Recht auf Privatheit im digitalen Zeitalter“ zu achten und zu schützen: http://www.un.org/depts/german/gv-sonst/a-c3-68-l45rev1.pdf.

Das Grundrecht auf vertrauliche Telekommunikation ist kein schrankenloses. Die Einschränkung des Telekommunikationsgeheimnisses darf nur aufgrund eines Gesetzes angeordnet werden (Art. 15 II Verf.). Das bedeutet, dass nur das Parlament, also die gewählten Volksvertreter, entscheidet, in welchen Fällen und Formen das Grundrecht eingeschränkt werden darf. Der Gesetzesvorbehalt bedeutet zudem, dass das Parlament nicht aus beliebigen Gründen das Grundrecht beschränken darf, sondern nur zur Ermittlung von schweren Straftaten und zur Gefahrenabwehr. Schließlich darf nur die Gerichtsbehörde (Art. 15 II Verf.) die Überwachung der Telekommunikation im Einzelfall ermächtigen. Der Richtervorbehalt dient zum Schutz der individuellen Freiheit, weil Richter „nur dem Gesetz“ (Art. 101 II Verf.) unterworfen sind. Richter sind unabhängig gegenüber der Regierung, den Parteien oder Lobbyisten. Bei „Gefahr in Verzug“ kann der Staatsanwalt die Überwachung vorläufig anordnen; sie muss aber innerhalb von 24 Stunden der Gerichtsbehörde mitgeteilt werden. Die Gerichtsbehörde muss die Überwachung innerhalb von 48 Stunden bestätigen. Tut sie dies nicht, gilt die vorläufige Überwachung als aufgehoben und die Abhörergebnisse dürfen nicht verwertet werden (Art. 267 II c.p.p.).

Art 15 Verf.

„(1) Die Freiheit und das Geheimnis des Schriftverkehrs und jeder anderen Form der Mitteilung sind unverletzlich.
(2) Ihre Einschränkung darf nur aufgrund einer begründeten Verfügung der Gerichtsbehörde unter gesetzlich bestimmten Garantien erfolgen.“

4.2.1.2 Wie läuft die Überwachung ab?

Zunächst muss ein begründeter Verdacht bestehen, dass eine bestimmte Person eine schwere Straftat plant oder begangen hat. Zu den schweren Straftaten zählt das Gesetz u. a. Mord, Drogenkriminalität, bandenmäßige und organisierte Kriminalität, Kinderpornographie, Terrorismus oder Geld- und Wertpapierfälschung (Art. 266 c.p.p.). Ist sich die Staatsanwaltschaft sicher, dass kriminelle Taten per Telefon abgesprochen werden, beantragt sie bei Gericht eine Telefonüberwachung. Die Gerichtsbehörde darf die Telefonüberwachung nur dann anordnen, wenn die Straftat nur auf diesem Wege aufgeklärt werden kann. Ist dies der Fall, ordnet sie mit einer „begründeten Verfügung“ (Art. 267 I c.p.p.) die Telefonüberwachung an. Auf der Grundlage dieser Verfügung fordert dann die Gerichtspolizei beim Mobilfunkanbieter oder Provider die Kommunikationsdaten der verdächtigten Person an. Telefonate oder der Internetverkehr können sodann von der Ermittlungsbehörde überwacht und mitgeschnitten werden.[152] Die Telefonüberwachung stellt später im Strafverfahren ein wichtiges Beweismittel dar.

152 Zur Vertiefung des technischen Ablaufs der Überwachung der Telefonate und des Internetverkehrs: Giovanni Nazzaro (2010): *Le intercettazioni sulle reti cellulari*, Fidenza.

Überwachung des Telefonats

Beim Telefonieren speichert der Mobilfunkanbieter zwei Arten von Daten. In einer ersten Datenbank werden die Bestandsdaten, also Name und Anschrift sowie Rufnummer (MSISDN), SIM-Kartennummer (IMSI) und PUK des Netzteilnehmers gespeichert. Durch die Abfrage der Bestandsdaten kann die Gerichtspolizei feststellen, wem das Handy gehört. In einer zweiten Datenbank speichert der Dienstanbieter die sogenannten Verbindungsdaten. Das sind Daten darüber, wer mit wem, wie lange, wann und wo telefoniert hat. Lokalisieren lässt sich das Handy über die genutzten Funkzellen. Wird das Handy eingeschaltet, verbindet es sich automatisch mit der nächstgelegenen Funkzelle. Auch wenn der Tatverdächtige nicht telefoniert, kann ihn die Ermittlungsbehörde orten. Dazu verschickt sie eine stille SMS. Diese wird nicht auf dem Display des Handys angezeigt, bewirkt aber, dass die gewünschten Standortdaten erzeugt werden.

Mobilfunkanbieter müssen die Verbindungsdaten bei Anrufen ohne Antwort für 30 Tage und bei Anrufen mit Antwort für 24 Monate speichern (Art. 132 D.lgs. 196/2003). Ruft beispielsweise ein Drogendealer regelmäßig eine Vielzahl von Kunden und einen Lieferanten an, kann die Gerichtspolizei über die Verbindungsdaten sein Kontaktnetzwerk mit Zeitleiste ermitteln und über die Bestandsdaten, wem die Handys gehören. Wechselt der Dealer als Abwehrmaßnahme etwa die SIM-Karte, kann das Telefon über die Gerätenummer (IMEI) identifiziert werden. Ist das Geschäftsmodell des Dealers durchleuchtet und sind die Hintermänner ausgeforscht, kann der Zugriff mit anschließender Hausdurchsuchung erfolgen, um beispielsweise nach verwahrten Drogen, Feinwaage, Tütchen und weiteren Handys zu suchen.

Fahnder können zur Identifizierung und Lokalisierung von Verdächtigten auch einen sogenannten IMSI-Chatcher einsetzen. IMSI-Catcher sind Geräte, die eine Funkzelle im Mobilfunknetz simulieren und die SIM-Kartennummer der Handys auslesen können. Befindet sich das abzuhörende Handy in der Nähe des IMSI-Chatchers, loggt es sich in die Funkzelle der Polizei ein. Nun kann jedes Telefonat mitgehört und mitgeschnitten werden. IMSI-Catcher sind rechtsstaatlich problematisch, weil damit auch die Möglichkeit besteht, Telefonate Unbeteiligter zu belauschen.

Überwachung des Internetverkehrs

Zur Telekommunikation zählt auch die Kommunikation über das Internet. Darunter fallen E-Mail-Nachrichten, Chats, Kommunikation über soziale Netzwerke sowie die Internettelefonie. Die Verbindung zum Internet stellt ein Provider zur Verfügung. Zugang zum Provider erhältst du aufgrund einer Zugangsberechtigung. Hierfür musst du zuvor einen Providervertrag abschließen, der die Bestandsdaten enthält, also deinen Namen und deine Anschrift. Verbindest du dein Smartphone mit dem Internet, weist der Provider deinem Smartphone eine sogenannte IP-Adresse zu. Rufst du nun eine Webseite auf oder versendest du eine E-Mail-Nachricht, protokolliert der Provider u. a. die IP-Adresse deines Smartphones und die des Webservers.

Nutzt du Internetdienste, fallen ebenso zwei Arten von Daten an, die Bestands- und die Verbindungsdaten. Provider sind verpflichtet, die Verbindungsdaten zwölf Monate zu speichern (Art. 132 D.lgs. 196/2003). Liegt ein Richterbeschluss vor, muss der Mailprovider den digitalen Briefkasten für die Fahnder öffnen. Wer Absender und Adressat der E-Mail-Nachricht mit illegalem Inhalt sind, erfahren die Fahnder den Providern, welche die entsprechenden Bestandsdaten vorrätig halten. Genauso kann der Mobber auf Facebook über die IP-Adresse und über seine Kontakte identifiziert werden, auch wenn er sich zur Verschleierung seiner Identität unter falschem Namen bei Facebook registriert und einloggt. Telefoniert der Verdächtigte über das Internet, etwa mit Skype, dann ist die Strafverfolgung aufwändiger. Denn das Skype-Telefonat wird verschlüsselt und kann deshalb von den Fahndern nicht so ohne Weiteres mitgeschnitten werden; es kann nur mithilfe von „digitalen Abhörwanzen" vor oder nach der Verschlüsselung belauscht werden.[153]

„Wir leben in einem Überwachungsstaat"

„Erstens, weil wir wollen, was uns vorgesetzt wird (…). Wir sind einverstanden, dass Facebook uns verfolgt (…). Zweitens, weil wir nicht wissen, dass wir getrackt werden (…). Und drittens, weil wir nicht aufmerksam sind. Wir ignorieren, dass Mobiltelefone nichts anderes als Ortungswanzen sind (…). Ich habe die Werkzeuge untersucht, die China, Syrien, der Iran, Ägypten, die USA und andere Staaten benutzen, um ihre Bürger auszuspähen – sie haben die Überhand in diesem Wettrüsten."

Bruce Schneier, Experte für Kryptographie

Vorratsdatenspeicherung: Pro und Contra

In Italien sind Mobilfunkanbieter für 24 und Provider für 12 Monate zur Vorratsdatenspeicherung verpflichtet. Verdachtsunabhängig müssen die Verbindungsdaten jedes Telefonats, jeder SMS samt Standortdaten sowie jeder E-Mail gespeichert werden; die Inhalte der Telefonate, der E-Mails oder der Chats werden nicht gespeichert. Den Ermittlungsbehörden ermöglichen die Verbindungsdaten, Kontaktnetzwerke von Kriminellen aufzudecken. Insbesondere Fahnder und Sicherheitsexperten sehen in der Vorratsdatenspeicherung ein probates Mittel zur Bekämpfung von Terrorismus und schweren Straftaten.[154]

Datenschützer und Bürgerrechtler warnen hingegen vor unverhältnismäßigen Eingriffen des Staates in die Telekommunikation. Aus den Verbindungsdaten kann nämlich ein lückenloses Bewegungs- und Verhaltensprofil

153 Branchenkenner bezweifeln, dass Skype abhörsicher ist: Torsten Kleinz (2013): *Wie abhörsicher ist Skype wirklich?* Zeit online, 31.07.2012 - 17:42 Uhr, http://www.zeit.de/digital/datenschutz/2012-07/skype-ueberwachung. Heise Security hat in einem Selbsttest festgestellt, dass Microsoft bei Skype mitlesen kann: http://www.heise.de/security/meldung/Vorsicht-beim-Skypen-Microsoft-liest-mit-1857620.html; http://www.heise.de/security/artikel/Mehr-Fakten-und-Spekulationen-zu-Skypes-ominoesen-Link-Checks-1865370.html; http://www.heise.de/security/meldung/PRISM-Ueberwachungskandal-Microsoft-ermoeglicht-NSA-Zugriff-auf-Skype-Outlook-com-Skydrive-1916340.html

154 Der Europäische Gerichtshof (EuGH) urteilte am 08.04.2014, dass die EU-Richtlinie zur massenhaften Speicherung von Telefon- und Internetverbindungsdaten aller Bürger ohne konkreten Anlass gegen EU-Recht verstoße. Die EU-Richtlinie verletze in gravierender Weise das Recht auf „Schutz personenbezogener Daten" und „Achtung des Privatlebens" und müsse deshalb auf das „absolut Notwendige" beschränkt werden: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054de.pdf.

der Bürger abgeleitet werden.[155] Bürger werden unter Generalverdacht gestellt, das Grundprinzip der Unschuldsvermutung wird damit außer Kraft gesetzt. Kritisiert wird auch die unverhältnismäßig lange Dauer der Vorratsdatenspeicherung.

Eine Alternative zur Vorratsdatenspeicherung wäre das Quick-Freeze-Verfahren, das einen Ausgleich zwischen dem Ermittlungsbedarf der Behörden und den Bürgerrechten schaffen würde. Mobilfunkanbieter und Internetdienstleister speichern zu Abrechnungszwecken Bestands- und Verbindungsdaten ihrer Kunden. Nach der Abrechnung werden die Verbindungsdaten gelöscht. Liegt ein Verdacht auf eine Straftat vor, können Fahnder in einem ersten Schritt die Löschung der Verbindungsdaten unterbinden und anordnen, dass die Daten vorübergehend, etwa für 7 Tage „eingefroren" werden. Erst in einem zweiten Schritt werden die Daten auf einen Richterbeschluss hin wieder „aufgetaut" und den Ermittlungsbehörden zur Strafverfolgung übermittelt.

„Wir überwachen jeden, überall"

The Gardian: *Ist es möglich, sich gegen staatliche Überwachung zu schützen?*

Edward Snowden: *Sie ahnen noch nicht einmal, was alles möglich ist. Das Ausmaß ihrer Möglichkeiten ist erschreckend. Wir können Apparate verwanzen. Ich kann Ihren Anschluss sofort identifizieren, sobald Sie sich eingewählt haben. Sie werden nie sicher sein, ganz egal, welche Sicherungsmaßnahmen Sie installieren.*

4.2.2 Überwachung durch NSA & Co.

Offenbar sind Geheimdienste in der Lage, Telefonate abzuhören, Chats, E-Mails oder SMS abzufangen, Daten abzugreifen, die populäre Apps über ihre Nutzer sammeln und ins Netz senden sowie Aktivitäten auf sozialen Netzwerken zu verfolgen. Die ab Juni 2013 veröffentlichten Dokumente des IT-Experten und NSA-Whistleblowers Edward Snowden legen nahe, dass NSA & Co. nach Belieben auch das kommunikative Verhalten von Bürgern fremder Staaten überwachen können.[156] Das ist eine neue Dimension der zwischenstaatlichen Spionage. Wird durch die weltweite Massenüberwachung Völkerrecht verletzt?

155 Daten-Experimente zeigen, dass sich aus Vorratsdaten sowie aus öffentlichen Facebook-Posts, Tweets und Blogeinträgen ein „fast vollständiges Abziehbild" über das Leben des Betroffenen erstellen lässt: http://www.nzz.ch/aktuell/digital/vorratsdaten-veroeffentlicht-nationalrat-balthasar-glaettli-1.18291061; http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten

156 Patrick Beuth (2013): Alles Wichtige zum NSA-Skandal, Zeit online, 28.10.2013 - 19:41 Uhr, aktualisiert 02.07.2015 - 08:59 Uhr, http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal; Forscher des kanadischen Citizen Lab haben in einem Bericht veröffentlicht, dass US-Spähtechnik in 83 Ländern eingesetzt wird, darunter auch in autoritären Regimen wie Iran, Syrien und Sudan: http://www.spiegel.de/netzwelt/netzpolitik/bluecoat-iran-und-sudan-filtern-internet-mit-us-technik-a-910268.html. Spähprogramme bietet offenbar auch die italienische Firma Hacking Team an autoritäre Staaten an: http://www.heise.de/security/meldung/Hacking-Team-Italienische-Schnueffelsoftware-in-zweifelhaften-Diensten-2117606.html; http://www.heise.de/security/meldung/Ueberwachungssoftware-Aus-Hacking-Team-wurde-Hacked-Team-2736160.html

4.2.2.1 Was erlaubt das Völkerrecht?

> *Sed quis custodiet ipsos custodies? Aber wer überwacht eigentlich die Überwacher?“*
>
> Juvenal, römischer Dichter

Staaten betreiben Spionage, um an geheime Informationen fremder Staaten zu kommen und die gewonnenen Erkenntnisse für nationale Zwecke zu verwerten. Das bloße Ausforschen ist völkerrechtlich nicht verboten, es tangiert nicht das Gewaltmonopol des Staates. Völkerrechtswidrig wäre, wenn die Staaten beim Spionieren die Territorialhoheit eines fremden Staates verletzen oder sich in dessen innere Angelegenheiten einmischen würden.[157] Beispiele dafür sind, wenn Spione Rebellen mit Waffen unterstützen, selbst Anschläge auf Infrastrukturen verüben, helfen Wahlergebnisse zu manipulieren oder Falschgeld in den Verkehr bringen.

Wie verhält sich das Völkerrecht zur neuen Art der Spionage, der Cyberspionage? Die Völkerrechtsexperten sind sich nicht einig. Einiges spricht dafür, dass das Völkerrecht keinen Schutz vor massenhafter Überwachung ausländischer Dienste bietet. Cyberspionage findet nämlich außerhalb des Hoheitsgebietes[158] fremder Staaten statt. Die NSA kann beispielsweise von ihrem Dienstsitz aus E-Mails abfischen, die über amerikanische Server geleitet werden oder Daten von Tiefseekabeln abzweigen, die sich in internationalen Gewässern befinden oder Telefonate über Spionagesatelliten abfangen, die im Weltall um die Erde kreisen.

Im Völkerrecht ist auch der Schutz der Privatsphäre der Bürger verankert. Ist Cyberspionage illegal, weil sie gegen die überall geltenden Menschenrechte verstößt? Der Bürgerrechtspakt von 1966 (IPbürgR)[159] sowie die Europäische Menschenrechtskonvention (EMRK)[160] schützen das Privatleben und die digitale Korrespondenz der Bürger. Der Schutz gilt aber nur für Personen, die der Hoheitsgewalt der Staaten unterstehen,[161] aber nicht gegenüber Menschen fremder Staaten. Die NSA handelt nach dieser Lesart nicht illegal, wenn sie die digitale Kommunikation der italienischen oder französischen Bürger überwacht. Nur wenn die Menschenrechte universelle Geltung hätten, dann wäre die umfangreiche Cyberspionage menschenrechtswidrig. Cyberspionage ist jedoch nicht straffrei. So droht das italienische Strafrecht jedem, der sich geheime Informationen für politische oder militärische Zwecke beschafft, mit fünfzehn Jahren Gefängnis.[162] Faktisch ist nationales Strafrecht hilflos gegenüber Cyberspionage. Für die Strafverfolgung ist der vollständige Nachweis der

157 Art. 2 Nr. 4, Nr. 7 UN-Charta
158 Das Staatsgebiet setzt sich zusammen aus der Landfläche, dem Küstenmeer, dem Boden sowie dem Luftraum. Die Begrenzung des Luftraums nach oben ist umstritten. Der Weltraum, der etwa in 100 km Höhe beginnt, zählt jedenfalls nicht mehr zum Gebiet irgendeines Staates.
159 Art. 17 IPbürgR
160 Art. 8 Abs. 1 EMRK
161 „Jeder Vertragsstaat verpflichtet sich, die in diesem Pakt anerkannten Rechte zu achten und sie allen in seinem Gebiet befindlichen und seiner Herrschaftsgewalt unterstehenden Personen (…) zu gewährleisten“ (Art. 2 Abs. 1 IPbürgR).
162 Art. 257 c.p.

einzelnen Straftat unerlässlich. In der Praxis ist es jedoch für Strafverfolgungsbehörden fast unmöglich, die Urheber einer professionellen Cyberspionage fremder Staaten gerichtsfest zu identifizieren.[163]

4.2.2.2 Schutzinstrumente vor Cyberspionage

Wie kann die beinahe ungehinderte Ausspähung durch NSA & Co. begrenzt oder sogar verhindert werden? Der „Krieg gegen den Terror" legitimiert weder NSA noch andere Dienste dazu, jeden Ort der Welt und jede digitale Kommunikation der Bürger zu überwachen. Ein freies und offenes Internet setzt den Schutz eines unverletzlichen Kerns der Privatsphäre voraus. Der Schutz kann durch Recht und Technik verbessert werden.

Menschenrecht auf vertrauliche Internetkommunikation (Vorschlag des Autors)

„(1) Jeder Mensch hat das Recht auf vertrauliche Internetkommunikation.
(2) Jeder Mensch hat das Recht, wirksame technische Maßnahmen einzusetzen, um abhörsicher zu kommunizieren.
(3) Jeder Staat fördert nach seinen Möglichkeiten die Entwicklung und den Einsatz technischer Maßnahmen zum Schutz vertraulicher Kommunikation.
(4) Ihre Einschränkung ist unzulässig, es sei denn auf Grund einer begründeten richterlichen Anordnung und nur in Fällen, die nationale Gesetze zum Schutz hochrangiger Rechtsgüter vorsehen. Die Anordnung muss unerlässlich sein und darf nur erfolgen, wenn ein konkreter Verdacht auf eine Straftat vorliegt.

- **Menschenrecht auf Privatsphäre:** Das Territorialdilemma der Menschenrechte lässt sich nur überwinden, wenn dieses von der Politik behoben wird. Die Europäische Union könnte sich für einen internationalen Vertrag stark machen, in dem ein verbesserter Schutz der digitalen Privatsphäre festgeschrieben wird. Das Menschenrecht auf Privatsphäre müsste direkt anwendbares Recht sein – also unabhängig vom Territorialprinzip auch außerhalb der Hoheitsgewalt der Staaten.
- **Schutz durch „Privacy by Design":** Datenschützer und IT-Experten fordern seit längerem schon, den Schutz privater Daten so früh wie möglich in IT-Technik einzubauen. Bereits bei der Entwicklung neuer Techniken und Anwendungen sollte der Datenschutz ein zentrales Thema sein. Zum Beispiel sollten App-Entwickler verpflichtet sein, IT-Konzepte zu wählen, welche die Vertraulichkeit der Kommunikation von vornherein sicherstellen, also Telefonate, E-Mails oder SMS standardmäßig verschlüsseln. Oder Cloud-Anbieter in Europa sollten IT-Verfahren mit den höchsten Sicherheitsstandards einsetzen, so dass Private und Unternehmen innerhalb eines abgeschirmten Bereiches vertraulich Daten austauschen können. Effektive Verschlüsselung sollte Standard in der Kommunikation über das In-

163 Die Geheimdienste folgen bei ihren Netzoperation der Devise der „plausible deniability". Das heißt, sie tarnen ihre Datenspionage und manipulieren Datenspuren so, dass sie ihre Aktionen stets glaubwürdig leugnen können. Cyberspionage kann auch unter „fremder Flagge" geführt werden. Vgl. Sandro Gaycken (2011): *Krieg der Rechner. Warum es so schwierig ist, sich vor militärischen Cyberangriffen zu schützen,* IP März/April 2011, https://zeitschrift-ip.dgap.org/de/article/getFullPDF/17647; Sandro Gaycken (2011): *Cyberwar. Das Internet als Kriegsschauplatz,* München

ternet sein. Gegenwärtig lässt sich das Recht auf Privatsphäre gegenüber professionellen Digitalspionen mit rechtlichen Instrumenten nicht durchsetzen. Für die Geheimdienste der Großmächte würde es schwieriger werden, massenhaft private Daten abzugreifen, wenn der Schutz der Privatsphäre zum Pflichtenheft für Anbieter neuer netzwerkfähiger Produkte, Apps und Software gehören würde.

- **Schutz von Whistleblowern:** Erst die Snowden-Enthüllungen haben das gesamte Ausmaß der weltweiten Cyberspionage durch NSA & Co. aufgedeckt. Whistleblower sollten deshalb die Möglichkeit haben, unabhängigen Medien geheime Informationen und Dokumente über abgesicherte Datenkanäle zukommen zu lassen. Journalisten prüfen darauf mit gebotener Sorgfalt, ob die Informationen zuverlässig sind, ob ein besonderes öffentliches Interesse an den geleakten Dokumenten besteht und achten darauf, dass Einzelpersonen durch die Veröffentlichung nicht gefährdet werden. Länder sollten Whistleblowern, die ihre Freiheit für den Schutz der Grundrechte aufs Spiel setzen, eine sichere Zuflucht gewähren.[164] Denn die Öffentlichkeit, die nicht über das Ausmaß der Datenspionage unterrichtet ist, kann die Massenüberwachung erst gar nicht auf den politischen Prüfstand setzen.

Der digitale Überwachungsstaat

- Sicherheit ist ein „Supergrundrecht", es hat Vorrang vor anderen Grundrechten
- Pflicht für Netzbetreiber zur Vorratsdatenspeicherung
- Präventive Überwachung der E-Mails, Chats oder Telefonate ohne konkreten Tatverdacht und richterlichen Beschluss
- Online-Durchsuchungen mithilfe von Staatstrojanern
- Zugriff in Echtzeit auf die Nutzerdaten der großen Datensammler, wie Google, Microsoft, Facebook oder Apple
- Zugriff der Behörden auf den privaten SSL-Masterkey von Internet-Firmen und Providern
- Recht der Behörden, die Bürger zur Herausgabe von Passwörtern unter Androhung von Haftstrafen zwingen zu können
- Verbot von Anonymisierungs-Apps, Prepaidkarten und anonymen E-Mail-Adressen
- „Nummernschild" bzw. persönliche IP-Adresse für jeden Internetnutzer (mit IPv6)

Europa fehlt die „technologische Souveränität" gegenüber den USA. Die Europäische Union muss deshalb den Aufbau einer eigenen IT-Industrie fördern, die Entwicklung sicherer Open-Source-Software gezielt unterstützen und eine eigene EU-Kryptozertifizierung einrichten. Quelloffene Software ermöglicht, dass sie ständig von einer Expertengemeinde überprüft werden kann, dass Sicherheitslücken regelmäßig geschlossen und absichtliche Schwachstellen identifiziert werden können. Nur ein digitaler Schutzschild kann offenkundig das Grundrecht der Bürger auf sichere Kommunikation gegenüber willkürlicher Massenüberwachung fremder Staaten gewährleisten. Eine bessere IT-Technik könnte Bürger in Europa freier machen.

164 Italien hat 2013 aus politischen Gründen einen Asylantrag Edward Snowdens abgelehnt. Die Verfassung sieht das Asylrecht lediglich für Ausländer vor, „denen im eigenen Lande die tatsächliche Ausübung der in der italienischen Verfassung gewährleisteten demokratischen Freiheit verwehrt ist" (Art. 10 Abs. 3). Die Voraussetzungen für Asyl fehlen, die USA ist zweifelsfrei ein demokratischer Staat. Müsste Italien Snowden an die USA ausliefern? Eine Auslieferung wäre wegen „politischer Straftaten" unzulässig (Art. 10 Abs. 4 Verf.). Offene Fragen: Sind Snowdens Enthüllungen als „politische Straftaten" zu bewerten? Kann ein Bürger auch in einem demokratischen Land politisch verfolgt werden?

4.2.3 Sicherheit vs. Privatsphäre

Der Konflikt Sicherheit oder Privatsphäre ist einer der zentralen politischen Konflikte im „informatisierten Alltag".[165]

Der Konflikt Sicherheit vs. Freiheit kann in einen digitalen Überwachungsstaat münden. Im digitalen Überwachungsstaat steht die nationale Sicherheit über den liberalen und demokratischen Bürgerrechten. Der einzelne Bürger ist faktisch machtlos; er bringt nicht mehr den Mut auf, gegen die Regierung zu opponieren und ein authentisches, autonomes Leben zu führen. Investigative Journalisten können nicht mehr so ohne Weiteres Straftaten wie Korruption von Regierungspolitikern oder Spitzenbeamten aufdecken, wenn der Schutz der Informanten und das Redaktionsgeheimnis nicht gewährleistet sind. Die Bürger werden anlass- und verdachtsunabhängig unter Generalverdacht gestellt und überwacht. Im Überwachungsstaat haben Bürger faktisch kein Grundrecht mehr auf „lauschfreie" Kommunikation. Verhindert die Regierung politischen Pluralismus, indem sie etwa eine „Warndatei" über politisch „suspekte" Blogger führt oder indem sie kritische Journalisten und Bürgerrechtler verfolgt und verhaftet, dann kippt der Überwachungsstaat zum autoritären Staat um.

Im Modell des digitalen Freiheitsstaates[166] dagegen ist das Grundrecht auf vertrauliche Kommunikation gewährleistet. IT-Experten beraten hier Bürger und Parlamentarier, damit sie aufgeklärte Entscheidungen treffen können. Auch im digitalen Freiheitsstaat muss entschieden werden, wie berechtigte Sicherheitsinteressen und Freiheitsrechte konkret ausbalanciert wer-

Der digitale Freiheitsstaat

- Grundrecht auf „Schutz der Privatsphäre" sowie auf anonyme und kryptographisch geschützte Telekommunikation
- Zertifizierung der kryptographischen Soft- und Hardware – ein Gütesiegel für Kryptoprodukte
- Überwachung der Telekommunikation nur bei klar definierten schweren Straftaten aufgrund eines begründeten Tatverdachts und eines richterlichen Beschlusses
- Verbot, unbemerkt und ungefragt Profile über Internetnutzer zu erstellen und mit Personendaten zu handeln
- Verbot der Vorratsdatenspeicherung
- Pflicht für die IT-Branche, ihre Kooperationen mit Behörden öffentlich zu machen
- Gebot für die Geheimdienste, die digitale Privatsphäre der Bürger anderer Staaten zu beachten
- Informantenschutz für Whistleblower
- Förderung der Medien- und Datenschutzkompetenz zum Schutz der Bürgerrechte

165 Alexander Roßnagel (2007): *Datenschutz in einem informatisierten Alltag,* Friedrich Ebert Stiftung, http://library.fes.de/pdf-files/stabsabteilung/04548.pdf; Nora S. Stampfl (2013): *Die berechnete Welt. Leben unter dem Einfluss von Algorithmen,* Hannover.

166 Digitaler Grundrechtekatalog: http://www.heise.de/tp/artikel/39/39197/s1.html
Digital Bill of Rights: http://ourdigitalrights.org/
The Crypto Anarchist Manifesto von Tim May: http://www.activism.net/cypherpunk/crypto-anarchy.html
Grundrechtscharta für das Internet von Jeff Jarvis: http://buzzmachine.com/2010/03/27/a-bill-of-rights-in-cyberspace; deutsche Übersetzung bei Zeit online: http://www.zeit.de/digital/internet/2010-03/jarvis-bill-of-rights
Gründungserklärung der Cypherpunks von Eric Hughes: http://www.activism.net/cypherpunk/manifesto.html;
Phil Zimmermann, Erfinder der E-Mail-Verschlüsselungssoftware PGP, fordert, dass Verschlüsselung zur „Bürgerpflicht" werden muss, soll die Gesellschaft vor einer „schlimmen Zukunft bewahrt werden": http://www.zeit.de/digital/datenschutz/2013-09/verschluesselung-interview-phil-zimmermann

den sollen, was den Bürgern auf längere Sicht die Freiheitsrechte wert sind und wie Ermittlungsbehörden und insbesondere Geheimdienste rechtsstaatlich und grundrechtlich gebändigt werden können.

4.3 Die Smartphone-Sicherheitseinstellungen

Das Smartphone ist eine der Sammelstellen persönlicher Daten und Medieninhalte, wie Telefonbuch, E-Mail-Nachrichten, SMS, Fotos und Videoclips. Solche Daten geben Auskunft über deine digitale Identität. Die Telekommunikation genießt zwar einen hohen Rechtsschutz, aber der alleinige Schutz durch Recht ist unzureichend. Wer das Telefonat sowie die Privatsphäre absichern will, ist auf Selbsthilfe angewiesen. So kannst du in einem ersten Schritt bereits mithilfe der Bordmittel für die Sicherheit deiner Privatsphäre sorgen.

Die grundsätzlichen Überlegungen zu Sicherheitsfragen gelten für alle Smartphones, unabhängig vom Betriebssystem. Die Kurzanleitungen beziehen sich auf das Samsung-Handy Galaxy S3 Mini, Android-Version 4.1.1.

Zugriffsschutz aktivieren

Gefahren: Ohne Zugriffsschutz kann jeder nach Belieben auf SMS, Telefonbuch, Anrufliste, unbeantwortete oder empfangene Anrufe auf deinem Smartphone zugreifen.

Sicherheitsmaßnahmen: Aktiviere in einem ersten Schritt die SIM-PIN, falls sie deaktiviert ist. Gehe dazu auf *Menü/Einstellungen/Sicherheit/SIM-Pin Optionen*. Unter SIM-PIN-Optionen kannst du bei Bedarf auch die SIM-PIN ändern. Schalte auch die Bildschirmsperre ein, wenn du das Handy gerade nicht benutzt. So geht’s: *Einstellungen/Sperrbildschirm/Sperrbildschirm*. Als Bildschirmsperre kannst du u. a. Gesichtserkennung, Musterabfrage, PIN-Code oder Passwort wählen. Entscheide dich für das Passwort, weil es die höchste Sicherheit bietet.[167] Hast du das Passwort vergessen, dann musst du dein Handy auf Werkeinstellungen zurücksetzen, um es wieder nutzen können. Das hat zur Folge, dass alle deine persönlichen Daten, Einstellungen und installierten Apps gelöscht werden. Damit dieser Fall nicht eintritt, sichere das Sperrmuster, den PIN-Code oder das Passwort auf einem externen Datenträger oder Zettel, den du an einem sicheren Ort verwahrst.

167 Ein gutes Passwort sollte mindesten 16 Zeichen lang sein, aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern bestehen. Wählst du hingegen die Musterabfrage, dann wechsle häufig die Richtung und wische regelmäßig das Display sauber, weil sich das Muster über die Fettspuren einfach nachvollziehen lässt: http://www.heise.de/security/meldung/Android-Muster-vorhersehbar-wie-Kennwoerter-2788675.html

WLAN und Bluetooth ausschalten

Gefahren: Offene WLAN- bzw. WiFi-Netze sind ohne Zweifel praktisch. Jeder kann sie am Bahnhof, im Café oder auf dem Stadtplatz nutzen, um seine E-Mails abzurufen oder um noch schnell im Internet eine Preisrecherche zu machen. Problematisch ist im fremden WLAN, dass sich eben jeder einloggen kann. Sind kriminelle Datendiebe in der Nähe des WLAN-Hotspots oder betreiben selbst einen öffentlichen Hotspot, können sie leicht die Zugangsdaten für dein E-Mail-Postfach oder Facebook-Konto abgreifen, weil die Daten bei einer unverschlüsselten Verbindung im Klartext zwischen WLAN-Hotspots und Smartphone ausgetauscht werden.

Sicherheitsmaßnahmen: Richte zuallererst ein sicheres WLAN mit WPA2[168] ein. Die Verschlüsselung durch den WPA2-Standard sorgt für die erforderliche Sicherheit der Datenübertragung. Der WEB-Standard gilt nicht mehr als sicher. Und so geht's: *Menü/Einstellungen/WLAN*. Nun erscheint eine Liste an WLAN-Routern, aus der du den gewünschten Router auswählen kannst. Ist der WLAN-Router aus Sicherheitsgründen abgeschaltet, musst du zuvor die Netz-SSID eingeben. Klicke hierfür auf den Eintrag *WLAN hinzufügen* und es erscheinen die Eingabefelder: *Netz-SSID*, also der Name des WLAN-Netzwerkes, *Sicherheit* und *Passwort*. Wähle unter *Sicherheit* den *WPA/WPA2 PSK*-Standard. Hast du den WLAN-Router ausgewählt oder hinzugefügt, dann setze ein Häkchen vor *Erweiterte Optionen anzeigen*. Im nächsten Dialogfenster kannst du, falls nicht bereits voreingestellt, die WLAN-Verschlüsselung mit WPA2 einrichten. Mit der Eingabe des Passwortes und dem Klick auf *Verbinden* hast du eine sichere Internetverbindung hergestellt.

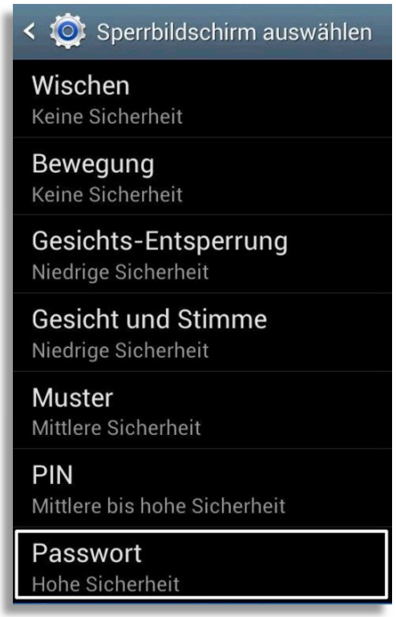


Abb. 22: Bildschirmsperre

Online-Banking oder Online-Einkäufe mit Kreditkarte solltest du nur in einer sicheren Umgebung tätigen.[169] Achte darauf, dass der Anbieter eine verschlüsselte Webseite benutzt. Eine solche erkennst du an der Protokollangabe „https://“ in der Adresszeile. Das „s“ steht für secure, kryptographisch sicher. Grundsätzlich solltest du über ein offenes WLAN so wenig wie möglich an vertraulichen Informationen senden oder abrufen, wie etwa Bankdaten oder Account-Daten für deine Webmails.[170]

168 Der ehemalige Standard für WLAN-Verschlüsselung WEP (Wired Equivalent Privacy) ist nicht mehr sicher. WEB-Verbindungen können beispielsweise mit der Aircrack-Software abgehört werden: http://aircrack-ng.org. Legal darf das Tool nur zum privaten Gebrauch genutzt werden. Wer es nutzt, um in fremde Netzwerke einzudringen, begeht eine Straftat: Art. 615ter c.p.

169 Bankgeschäfte solltest du unter Windows über ein eigenes Benutzerprofil mit geringen Administratorenrechten abwickeln. Tools für sicheres Online-Banking: BitBox von Sirrix (http://www.sirrix.de/content/pages/BitBox.htm); c't Bankix von Heise Online (http://www.heise.de/download/ct-bankix.html).

170 Unterwegs solltest du E-Mails nur über (sichere) Hotspots deines Mobilfunkanbieters oder über deine Mobilfunkverbindung abrufen; Webseiten einer Online-Zeitung hingegen kannst du unbesorgt auch über ein öffentliches WLAN aufrufen.

Deaktiviere nach dem Gebrauch das offene WLAN, damit sich das Smartphone nicht automatisch ins Funknetz einwählt, wenn du in die Nähe des Cafés kommst, wo du dich kürzlich eingewählt hast. WLAN ausschalten geht so: *Menü/Einstellungen/WLAN*. Über den Schieberegler kannst du WLAN deaktivieren oder aktivieren. Befindet sich der Schieberegler auf der rechten Seite, hat er eine grüne Farbe und ist aktiviert. Befindet er sich auf der linken Seite, ist er ausgegraut und deaktiviert. Am besten ist, wenn du den benutzten WLAN-Router aus der Liste der verwendeten Verbindungen löschst, damit keine unkontrollierte Verbindung zum Internet hergestellt werden kann. Hierfür musst du den benutzten WLAN-Router markieren und auf die Schaltfläche *Entfernen* drücken. Dasselbe gilt für den Kurzstreckenfunk Bluetooth; aktiviere ihn nur für den Bedarfsfall, damit Unbefugte darüber nicht auf das Internet zugreifen können. Ausschalten kannst du Bluetooth, so wie das WLAN, mithilfe des Schiebereglers: *Menü/Einstellungen/Bluetooth*. abrufen

Du kannst dein Smartphone als mobilen WLAN-Router auch selbst nutzen und für WLAN-fähige Geräte freigeben, beispielsweise für ein Notebook. Schalte nach dem Gebrauch den mobilen Hotspot aus, damit Kriminelle keine Chance haben, dein Smartphone für Straftaten im Netz zu missbrauchen. Einrichtung und Deaktivierung des mobilen Hotspots findest du unter: *Menü/Einstellungen/… Weitere Einstellungen*.

Software regelmäßig updaten

Gefahren: Das Betriebssystem deines Smartphones, ob Android, iOS oder Windows Phone, kann Sicherheitslücken aufweisen. Über bekannte Sicherheitslücken kann dein Smartphone mit Schadcode infiziert und deine Daten können manipuliert, zerstört oder ausspioniert werden.

Sicherheitsmaßnahmen: Führe deshalb als Sicherheitsmaßnahme regelmäßig die vom Gerätehersteller empfohlenen Software-Updates durch. Willst du Geld sparen, kannst du die Sicherheitsupdates auch über den PC von der Webseite des Geräteherstellers herunterladen und per Synchronisierungssoftware auf das Smartphone überspielen. Gerätehersteller bieten eine solche Synchronisierungssoftware kostenlos an.

Schadcode kann allerdings nicht nur über eine Sicherheitslücke des Betriebssystems auf dein Smartphone gelangen, sondern auch über eine der installierten Apps. Halte deshalb deine Apps stets aktuell.

4.4 Vorsicht bei Apps

4.4.1 Apps als Datensammler

In der Regel greifen Android-Apps auf vertrauliche Daten zu, die sie eigentlich nicht benötigen. Zu den begehrten Informationen der Datensammler zählen E-Mail-Adressen, Telefonnummern, die IMEI-Nummer, Standortdaten,[171] Betriebssystem sowie installierte Apps. Lesen Apps auch die Daten aus dem Facebook-Profil aus, entsteht ein detailliertes Profil des Nutzers: Wer er ist, welche Interessen er hat, was er sich gekauft hat, wo er wohnt, arbeitet oder sich gerade aufhält. Kritisch an der Datenabfrage ist, dass sie vielfach ohne Wissen und Erlaubnis des Nutzers erfolgt.[172] Welche Daten erforderlich sind, damit die App ihren Dienst erfüllen kann, hängt von der Art des Dienstes ab. Eine App, die etwa das nächste Fischrestaurant am Urlaubsort anzeigt, benötigt fraglos die Positionsdaten des Nutzers, aber nicht die hochsensible IMEI-Nummer. Erfolgt der Datenzugriff heimlich, liegt ein klarer Verstoß gegen den italienischen Datenschutzkodex vor. Persönliche Daten dürfen nämlich nur mit informierter Zustimmung des Betroffenen erhoben und verwendet werden. Datenschutzkonform wäre, wenn der Nutzer jederzeit jede einzelne Berechtigung einer App an- und ausschalten könnte.

Checkliste App-Datenschutz

- Werden bei der App-Installation alle Rechte angezeigt, die eine App anfordert?
- Hat der Nutzer bei der Installation der App die Option die angeforderten Zugriffsrichte zu akzeptieren oder abzulehnen?
- Sammelt die App auch Daten, die nicht für ihre Funktion erforderlich sind? Wenn ja, welche?
- Werden die Daten anonymisiert und verschlüsselt ins Netz übertragen?
- An wen werden die Daten gesendet, an App-Entwickler, Datenhändler oder Analysenetzwerke?
- Für welche Zwecke werden die gesammelten Daten verwendet, nur firmenintern zu statistischen Zwecken oder für personalisierte Werbung?

4.4.2 Schutz vor Schnüffel-Apps

Was kann man dagegen tun, wenn zumeist kostenlose Apps persönliche Daten ungefragt an die App-Entwickler oder Werbenetzwerke senden? Zum Schutz deiner Privatsphäre solltest du nicht wahllos Apps installieren. Kontrolliere vor der Installation einer App, welche Berechtigungen die App einfordert. Suche im Netz nach

171 Die Art und Weise, wie sich Menschen bewegen, ist offenbar „sehr einzigartig“. Einem Forscherteam des Massachusetts Institute of Technology (MIT) ist es gelungen, mit sehr wenigen Bewegungsdaten Handynutzer zu identifizieren. Lediglich mit vier zufällig ausgewählten Angaben zu Ort und Zeitpunkt sind 95 Prozent der Handynutzer erkennbar, mit höchstens elf Bewegungsdaten bereits jeder: http://www.taz.de/Bewegungsdaten-von-Mobiltelefonen/!113867/

172 „Telefoniert-nach-hause.de“ ist ein Wiki, das Informationen darüber sammelt, welche Daten Apps ungefragt von Smartphones abgreifen: https://www.telefoniert-nach-hause.de/

zuverlässigen Tests, etwa von Verbraucherzentralen, Technikzeitschriften oder IT-Experten, die darüber informieren, ob die gewünschte App eine Datenkrake ist. Ein weiterer Kritikpunkt ist das Handling von App-Berechtigungen unter Android. Android-Handys kennen keine individuelle Rechteverwaltung. Installieren Nutzer eine Android-App, haben sie nur die Wahl den angeforderten Rechten im Paket zuzustimmen oder auf die App gänzlich zu verzichten.

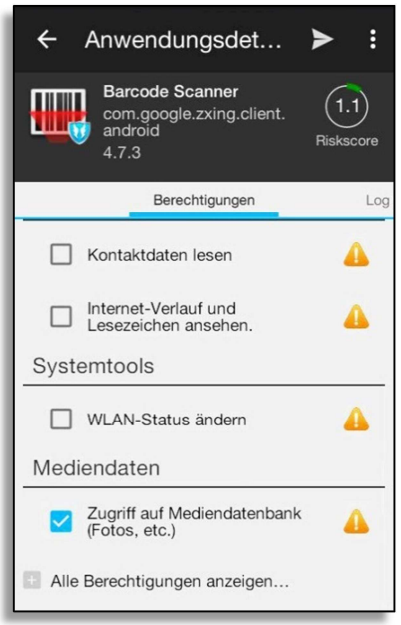


Abb. 23: Weniger Rechte für Barcode Scanner

Technische Schutzmaßnahmen

Mehr Kontrolle ermöglicht die Privacy-App SRT AppGuard.[173] Mit ihrer Hilfe können Nutzer einfach die Zugriffsrechte ausgewählter Apps nachträglich beschränken und so selber entscheiden, welche Daten sie preisgeben wollen. Da die App nicht im Google Play Store erhältlich ist, musst du die APK-Datei von der Webseite des Anbieters[174] auf das Handy herunterladen. Bevor du die Anti-Spionage-App installierst, musst du sicherstellen, dass die Option *Unbekannte Quellen* in den Android-Einstellungen aktiviert ist.

Starte AppGuard und du gelangst zur App-Übersicht, in der eine Liste aller installierten Apps angezeigt wird. Ein Risk-Score kennzeichnet Apps mit besonders vielen Zugriffsrechten. Wähle die suspekte App und setze sie auf die Überwachungsliste. Tippe dazu auf die Schaltfläche *Überwachen* und die App wird deinstalliert, modifiziert und automatisch wieder installiert. Der Nachteil überwachter Apps ist, dass alle gespeicherten Einstellungen, wie Spielefortschritte, verloren gehen. Außerdem erhalten überwachte Apps nicht mehr Updates vom Google Play Store. AppGuard bietet indes die Alternative an, selbst nach Updates für überwachte Apps zu suchen. Damit AppGuard prüfen kann, ob Updates zur Verfügung stehen, benötigt die App Zugriff auf dein Google-Konto. Sind Updates für die überwachten Apps verfügbar, werden sie automatisch heruntergeladen, gepatcht und installiert. Dabei bleiben alle Daten der App erhalten.

Bei überwachten Apps zeigt AppGuard eine Übersicht aller angeforderten Zugriffsrechte an. Du kannst nun der App manuell alle Berechtigungen entziehen, die du ihr nicht einräumen willst. Bedenke, dass Apps ohne bestimmte Rechte nicht mehr funktionieren. Eine Staumelder-App muss beispielsweise Zugriff auf das Internet haben und auf die GPS-Positionsdaten zurückgreifen können, soll sie den Fahrer rechtzeitig vor einem Stau warnen. In der Kategorie *Netzwerkkommunikation* befindet sich hinter *Vollständiger Internetzugriff* ein Schraubenschlüssel. Tippst du darauf, öffnet sich eine Liste mit allen Webservern, mit denen die

173 Den „digitalen Türsteher“ SRT AppGuard haben Informatiker des Zentrums für IT-Sicherheit an der Universität Saarbrücken entwickelt: http://www.deutschlandfunk.de/die-aufpasser-app.684.de.html?dram:article_id=214240
174 http://www.srt-appguard.com/de/

überwachte App Daten austauscht. Hier kannst du auch einstellen, mit welchen Webservern sich die App verbinden darf und mit welchen nicht.

4.5 Schutz vor Viren & Co

Gefahren: Schadcode fangen sich Smartphone-Nutzer grundsätzlich auf zwei Wegen ein. Erstens, Viren gelangen über Sicherheitslücken des Betriebssystems oder eine unprofessionell programmierte App auf das Handy. Eine besondere Gefahrenquelle stellen hierbei die Browser dar, sie stellen die Verbindung mit den Webseiten her. Hinter Webinhalten kann sich Schadcode verbergen, der über Sicherheitslücken des Browsers auf dein Handy eingeschleust werden kann. Zweitens, der Anwender wird dazu verleitet, selbst die Viren auf seinem Smartphone zu aktivieren. Das kann passieren, indem du voreilig einen Mail-Anhang öffnest. In einer .zip- oder .exe-Datei im Anhang können sich auch Trojaner verbergen. Links in einer Betrugsmail können zu einer manipulierten Webseite führen, die eine Sicherheitslücke des Webbrowsers ausnutzt, um darüber einen Trojaner auf das Handy zu befördern. Schadcode kann auch über infizierte Apps aufs Handy gelangen oder im schlimmsten Fall bereits ab Werk mit an Bord sein. Infizierte Handys spionieren das Nutzerverhalten aus, versenden u. U. kostenpflichtige Premium-SMS oder rufen teure Telefonnummern an. Den Schaden bemerken die Nutzer erst bei der nächsten Telefonrechnung oder beim nächsten Aufruf ihres Online-Kontos.[175]

Sicherheitsmaßnahmen: Die besten Abwehrmaßnahmen vor Viren sind eine Kombination aus Update-Management, umsichtigem Nutzer-Verhalten und dem Einsatz von effizienten Virenscannern. Spiele stets die neuesten Sicherheitsupdates ein, insbesondere die für Browser und Apps, dann haben es Angreifer schwerer, an deine Daten heranzukommen. Öffne keine E-Mail-Anhänge, die von unbekannten Absendern mit dubiosem E-Mail-Text stammen. Klicke auch nicht auf jeden Link in deiner E-Mail; der Link könnte auf manipulierte Webseiten führen, über die du Schadcode auf dein Handy holst. Lade dir nicht jede Spiele-App auf dein Handy; hinter dem Spiel kann sich krimineller Programmcode verbergen, der Tür und Tor zu deinem Handy öffnet, neue Schadsoftware nachlädt, dein Handy in einen Zombie verwandelt oder für Abzocker eine wunderbare Brotvermehrung wird. Lade nur Apps von vertrauenswürdigen App Stores herunter,[176] recherchiere, was andere Nutzer

175 Mehr zu den gemeinen Gefahren der Smartphone-Viren: Ulf Schönert (2013): *Attacke aufs Handy,* Zeit online, 19.06.2012 - 13:53 Uhr, http://www.zeit.de/zeit-wissen/2012/04/Smartphones; heise Security: http://www.heise.de/security/meldung/Hochentwickelte-Android-Trojaner-ins-Netz-gegangen-1885163.html; http://www.heise.de/security/meldung/Vorinstallierte-Spionagesoftware-auf-China-Smartphones-2221792.html

176 Offizielle App-Stores sind keine Gewähr für eine virenfreie Zone: http://www.heise.de/security/meldung/32-Abzock-Apps-bei-Google-Play-1846209.html; http://www.heise.de/security/meldung/mTAN-Trojaner-via-SMS-und-Google-Play-1858695.html

von der App halten; so verminderst du das Risiko, dass deine Daten ausspioniert und missbraucht werden können.

Ein Virenscanner gehört zur Grundausstattung eines jeden Smartphones, denn Smartphones sind mobile PCs mit Telefon- und Internetanschluss. Antivirenprogramme überprüfen in regelmäßigen Abständen installierte Apps, das Betriebssystem und abgelegte Daten auf Schadcode,[177] scannen E-Mail-Anhänge und warnen vor unsicheren Webseiten.[178] Einige Virenscanner bieten auch einen Diebstahlschutz (Anti-Theft) an. Geht dein Smartphone verloren, kannst du es damit aus der Ferne orten, sperren und Daten löschen.[179]

Antiviren-Apps, die im letzten Jahr noch sämtliche Schädlinge im Test erkannt haben, können in diesem Jahr schlechtere Testwerte liefern. Bevor du eine Antiviren-App installierst, sollst du dir die Testergebnisse der Virenlabore[180] ansehen oder einen Blick auf die Bestenliste der Virenscanner bei bekannten Security-Webseiten[181] werfen.

Hersteller	Produkt	Webseite
AVAST Software	avast! Mobile Security	https://play.google.com/store
AVG Mobile technologies	AVG Antivirus Free	https://play.google.com/store
AVIRA	Avira Free Android Security	https://play.google.com/store
Lookout Mobile Security	Lookout Security & Antivirus	https://play.google.com/store
Panda Security	Panda Cloud Antivirus	https://play.google.com/store
TrustGo Inc.	Antivirus & Mobile Security	https://play.google.com/store
ZONER Inc.	Zoner AntiVirus Free	https://play.google.com/store

Tab. 12: Freeware Virenscanner

177 Android-Virenscanner bieten keinen vollständigen Schutz, offenbar haben Cyberkriminelle leichtes Spiel Virenscanner auszutricksen: http://www.heise.de/security/meldung/Android-Virenscanner-sind-leicht-auszutricksen-1855331.html

178 Die Safe-Browsing-Funktion schützt Nutzer vor Webseiten, die Schadcode enthalten oder gefälscht sind (Phishing-Webseiten). Das Fachmagazin „c’t“ berichtete, dass manche Antiviren-Apps durch den Browserschutz mehr Informationen zum App-Hersteller senden als nötig. Ist dir der Privacy-Schutz wichtiger als der Virenschutz, dann schalte den Browserschutz aus: Ronald Eikenberg (2014): *Virenschutz sticht Datenschutz. Android-Virenscanner telefonieren nach Hause,* in: c’t 2014, Heft 6, S. 52.

179 Die Anti-Diebstahl-Funktionen schützen lediglich vor Gelegenheitsdieben, gegen Profis sind sie hilflos. Profis schalten die Mobilfunk- und WLAN-Verbindung ab, sodass das Handy weder per SMS noch übers Internet erreichbar ist. Liegen die Handydaten auf der microSD-Karte, kann der Dieb diese einfach herausnehmen und kommt so trotz Anti-Diebstahl-Funktion an die Daten heran. Wirklichen Schutz bietet nur eine Verschlüsselung der Daten in Verbindung mit einer guten Backup-Strategie.

180 AV-Test: http://www.av-test.org/tests/; AV-Comparatives: http://www.av-comparatives.org/

181 Heiße Security: http://www.heise.de/security

4.6 Schutz der Privacy

Gefahren: Verlierst du dein Handy, hat der Finder Zugriff auf Fotos, Videos, Adressbuch, SMS, WLAN-Zugangsdaten, Notizen, E-Mails oder Surfverlauf im Browser. Hast du deine Daten auf einer microSD-Karte gespeichert, benötigen Neugierige lediglich einen Kartenleser, um deine Daten zu einzusehen und zu kopieren. Ist dein Handy ungesichert, können Kriminelle einfach eine Spionage-App installieren und so deine Telefonate und deinen Internetverkehr belauschen.[182] Neugierige können dein Surfverhalten über die Chronik und die Surfspuren, welche dein Browser hinterlässt, rekonstruieren.

Sicherheitsmaßnahmen: Willst du deine persönlichen Daten auf dem Smartphone effektiv schützen, musst du sie verschlüsseln. Seit Version 3.0 kannst du deine Daten mit Android-Bordmitteln verschlüsseln;[183] du kannst deine digitale Privatsphäre auch mit Verschlüsselung-Apps vor unberechtigten Zugriffen schützen.

Willst du dein Handy eines Tages entsorgen, verschenken oder verkaufen, dann solltest du deine persönlichen Daten wirksam shreddern. Mithilfe von Datenrettungstools können die vermeintlich gelöschten Dateien auf deiner microSD-Karte wieder hergestellt werden und sind so für Unberechtigte lesbar. Ebenso solltest du dein Smartphone von Datenspuren wirksam säubern, die Rückschlüsse auf deine Handy-Tätigkeiten ermöglichen – wie, welche Webseiten du aufgerufen hast. Den „Schwarzen Gürtel" in digitaler Privatsphäre gibt es nicht. Du kannst aber Werkzeuge zur digitalen Selbstverteidigung einsetzen und dich über Risiken bei ihrer Nutzung auf dem Laufenden halten.[184]

„Der beste Schutz für den Menschen (…) besteht in einer freien, offenen und toleranten Gesellschaft."

Michael Seemann, Blogger

„Es gibt einen Grund, warum diese Daten für Wirtschaft und Politik wertvoll sind: Information ist Macht. Und wenn jemand anderes deine Daten hat, du aber keine von ihm, dann hast du gerade einen großen Teil deiner politischen Macht geopfert."

Daniel Suarez, Softwareentwickler und Autor

Art. 17 IPbürR

„(1) Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben (…) und seinen Schriftverkehr (…) ausgesetzt werden."

Art. 8 EMRK

„(1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs."

182 Reporter sind in Gefahr, wenn sie Apps nutzen, die brisante Fotos, Videos oder Dokumente unverschlüsselt an die Redaktion senden. Für Hacker und Behörden ist es dann einfach, das Recherchematerial bereits vor der Veröffentlichung auszuspähen. Eine Gefahr besteht insbesondere in Ländern, in denen Behörden die Presse überwachen.

183 Jürgen Schmidt u. a. (2013): *Unter Verschluss. Android-Geräte verschlüsseln,* c't 2013, Heft 4, S. 136-138.

184 Nur „gute Kryptographie" schützt noch vertrauliche Daten. Der US-Geheimdienst NSA und der britische Dienst GCHQ können offenbar einen Großteil des verschlüsselten Datenverkehrs im Internet mitlesen: http://www.heise.de/security/meldung/NSA-und-GCHQ-Grossangriff-auf-Verschluesselung-im-Internet-1950935.html

4.6.1 Betriebssystem und lokale Daten verschlüsseln

4.6.1.1 Android verschlüsseln

Lade zunächst den Akku voll auf und lasse das Ladegerät am Stromnetz. Wähle nun ein Passwort für Verschlüsselung und Sperrbildschirm. Wähle ein sicheres Passwort, denn der Schutz deiner Daten ist so sicher wie das gewählte Passwort. Android ermöglicht Passwörter mit einer Länge von maximal 16 Zeichen, die aus Zahlen, Buchstaben und Sonderzeichen zusammengesetzt sind. Willst du Sicherheit, musst du das Eintippen langer und komplexer Passwörter in Kauf nehmen. Standardmäßig werden nur die Daten des internen Speichers verschlüsselt. Das System, die Apps und die Daten auf der externen microSD-Karte bleiben ungeschützt. Wird auch die microSD-Karte verschlüsselt, bleiben die Dateinamen dennoch lesbar. Ein Angreifer kann in diesem Fall nicht auf die Inhalte der Dateien zugreifen, aber eventuell Rückschlüsse vom Dateinamen auf den Inhalt ziehen, wie etwa bei „spielwetten.doc“ oder „onlinebanking.pdf“.

Checkliste Crypto-App

- Handelt es sich bei der App um eine Open-Source-Anwendung?
- Wurde der Code von unabhängigen Crypto-Experten überprüft?
- Zählt die verwendete Verschlüsselungstechnik zu den anerkannten Crypto-Standards?
- Unterstützt die App eine Ende-zu-Ende-Verschlüsselung?
- Fallen bei der Nutzung Metadaten an – also wer hat wo und wann mit wem kommuniziert?

Die Verschlüsselung kannst du unter *Menü/Einstellungen/Sicherheit/Gerät verschlüsseln* aktivieren. Tippe hierfür auf die Schaltfläche *Gerät verschlüsseln*, gib das Passwort ein und tippe *Weiter*. Tippst du erneut *Gerät verschlüsseln*, wird die Verschlüsselung gestartet. Nach einiger Zeit ist der Vorgang abgeschlossen. Zukünftig werden erst nach der Eingabe des Passwortes deine Daten entschlüsselt und lesbar. Beachte: Hast du dein Handy verschlüsselt, kannst du die Verschlüsselung nicht mehr rückgängig machen – du kannst es nur mehr auf Werkeinstellung zurücksetzen.

4.6.1.2 Lokale Daten verschlüsseln[185]

Mit EDS[186] (Encrypted Data Store) lassen sich verschlüsselte Datencontainer erstellen. Die Wahl fiel auf EDS, weil die App Sicherheitsstandards nutzt, die von US-Regierungsbehörden verwendet werden, um Dokumente mit bis zu höchster Geheimhaltung zu schützen. Ein Angreifer kann damit weder Dateiinhalte noch Ver-

185 Das Grundrecht auf vertrauliche, private Kommunikation (Art. 15 Verf.) gilt nicht für Daten, die auf dem PC oder Smartphone gespeichert sind; diese unterliegen lediglich dem Datenschutzkodex (D.lgs. 196/2003).
186 EDS wird in Google Play angeboten; Webseite des Entwicklers: http://www.sovworks.com

zeichnisstruktur und Dateinamen erkennen. Außerdem können die mit EDS erstellten Containerdateien am PC mit dem Verschlüsselungstool VeraCrypt[187] geöffnet werden. Der Autor hat sich für die Bezahlversion entschieden, weil sie mehr Funktionen bietet als die kostenlose App EDS Lite und weil er Entwickler unterstützen will, die Security-Apps für „alle“ anbieten.[188]

Datentresor erstellen

Das Handling der EDS-App ist einfach. Öffne die App und lege einen neuen Datencontainer an. Tippe hierzu oben rechts im Bildschirm auf das Schlüssel-Symbol. Im nächsten Fenster stehen die Optionen *Create standard container* und *create hidden container* zur Auswahl. Der Standard Container ist für andere sichtbar. Mit *create hidden container* könntest du innerhalb eines sichtbaren Containers einen versteckten anlegen. Es kann nämlich der Fall eintreten, dass du gezwungen wirst, das Passwort für deinen verschlüsselten Container herauszugeben. Kopierst du in den äußeren Container nur ein paar „unwichtige“ Daten, gibt sich der Angreifer mit diesen zufrieden. Der innere, für den Angreifer unsichtbare Container, bleibt so vor unberechtigten Zugriffen geschützt. Auf dem Handy dürfen für diesen Fall aber auch keine Datenspuren zu finden sein, die auf einen „unsichtbaren“ Datentresor hindeuten.

Abb. 24: Datencontainer erstellen

Tippe *Create standard container* und wähle unter *Select path* deine microSD-Karte als Speicherort des Datentresors aus. Lege unter *Enter file name* den Namen für den neuen Container fest und bestätige mit *Select*. Den voreingestellten Verschlüsselungsalgorithmus und Hashalgorithmus kannst du übernehmen. Zum Abschluss legst du noch die Dateigröße fest und wählst zum Schutz des Datentresors ein starkes Passwort oder eine Schlüsseldatei aus. Das Passwort sollte eine Mindestlänge von 16 Zeichen haben sowie aus Groß-, Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Mit *OK* wird der neue Datencontainer erstellt. In deinem Dateimanager erscheint dein Datentresor wie eine normale Datei, du kannst sie also kopieren, verschieben oder auch löschen.

Die Konfiguration des Datentresors kannst du auch im Nachhinein ändern. Öffne hierfür die Crypto-App, halte den Finger auf den Container gedrückt und wähle in der Auswahl *Container settings*. Der Rest ist selbsterklärend.

187 Produktwebseite: https://veracrypt.codeplex.com; Tutorial: https://veracrypt.codeplex.com/wikipage?title=Beginner%27s%20Tutorial
188 EDS und die kostenlose Version EDS Lite werden in Google Play angeboten.

Datencontainer einbinden und verwalten

Als Nächstes musst du den angelegten Datentresor einbinden (mounten), damit du alle deine privaten Daten dorthin verschieben kannst. Öffne EDS, tippe oben rechts auf die Pinn-Nadel, navigiere dich bis zum Speicherort des Containers durch und bestätige mit *Select*. Darauf fordert dich EDS auf, das Passwort einzugeben – kurz darauf ist der Datentresor geöffnet.

EDS hat einen internen Dateimanager. Oben rechts im Bildschirm befinden sich seine drei Symbole: *New folder*, *Browse device* und *Multi select*. Mit *New folder* kannst du im Container einen neuen Ordner anlegen. Mit *Browse device* navigierst du zum Speicherort deiner Dateien. Mit *Multi select* kannst du mehrere Dateien anklicken und kopieren.

Wie kopiert man nun beispielsweise vertrauliche Fotos in den Tresor? Navigiere zum Speicherort deiner Fotos, in der Regel *extSdCard/DCIM/Kamera* und setze ein Häkchen vor dem Ordner oder den Fotos, die du in den Datentresor kopieren willst. Tippe jetzt auf das Schloss-Symbol – oben rechts im Bildschirm und du bist wieder im EDS-Container. Tippe nun auf *Menü* und in der Auswahl auf *Einfügen*. Kurz darauf sind deine Fotos im Datentresor.

Tipp

Bequemer kannst du via VeraCrypt Daten in den EDS-Container kopieren. Du musst dazu nur die microSD-Karte in den PC einstecken und den EDS-Container in Windows „einbinden".

Sollen deine Fotos aus dem Container entfernt werden, dann tippe auf *Menü* und in der Auswahl auf *Multi select* oder oben rechts auf das Multi select-Symbol. Setze nun bei allen Fotos oder Ordnern, die du löschen willst, ein Häkchen. Gehe nochmals auf die *Menü*, tippe in der Auswahl auf *Delete* und bestätige mit *Yes*.[189]

Willst du den Datentresor wieder verschließen, dann halte den Finger auf den Datencontainer gedrückt und wähle in der Auswahl *Close container*. Über die Menü-Taste und *Stopp Service and exit* steigst du aus der App aus.

189 Sollen auf der microSD-Karte weder Fotos noch Fotospuren zu finden sein, musst du dort die Fotos löschen und den freien Speicher mit Löschtools wie CCleaner (http://www.piriform.com/ccleaner/download) oder Eraser (http://eraser.heidi.ie/download.php) sicher löschen.

4.6.2 Datenverkehr verschlüsseln

Für den wirksamen Schutz der digitalen Privatsphäre ist Verschlüsselung unumgänglich. Verschlüsselung ist der digitale Schutzschild des Grundrechts auf „informationelle Selbstbestimmung“. Verschlüsselte Kommunikation stellt sicher, dass die Nachricht nur für denjenigen les- oder hörbar ist, für den sie bestimmt ist; dass der Kommunikationspartner wirklich die Person ist, als die sie sich ausgibt und dass die Nachricht auf dem Weg vom Absender zum Empfänger nicht verändert wird. Apps wie Threema, RedPhone oder K-9 Mail und OpenKeychain leisten hierfür nützliche Dienste. Sollen die Daten auch auf dem Smartphone vor unberechtigten Zugriffen sicher sein, musst du Android komplett verschlüsseln oder Crypto-Apps wie EDS für verschlüsselte Datencontainer einsetzen.

4.6.2.1 Chat verschlüsseln

Einige Chats sind nur für den Kommunikationspartner bestimmt, etwa ein Chat mit einem Anwalt oder mit einem investigativen Journalisten. Threema[190] oder Hoccer[191] sind Crypto-Messenger, die standardmäßig Nachrichten Ende-zu-Ende verschlüsseln, sodass selbst Serverbetreiber oder Hacker auf die Chat-Inhalte keinen Zugriff haben.

Wie funktioniert Threema? Die App erzeugt ein Schlüsselpaar aus privatem und öffentlichem Schlüssel. Die Kurznachricht wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und mit dem privaten Schlüssel des Empfängers wieder entschlüsselt. Die Chat-Partner müssen jedoch zuvor ihre öffentlichen Schlüssel ausgetauscht haben. Bei der asymmetrischen Verschlüsselung muss sichergestellt sein, dass der Empfänger der Nachrichten auch wirklich derjenige ist, als der er sich ausgibt. Threema kennt bei der Überprüfung der Kontakte verschiedene Vertrauensstufen. Höchstes Vertrauen wird erreicht, wenn man den öffentlichen Schlüssel bei einem persönlichen Treffen austauscht. Dazu gibt man entweder die Threema-ID des Kontaktes manuell ein oder fotografiert gegenseitig den QR-Code direkt vom Handy-Display ab. Die höchste Sicherheitsstufe wird von der App mit „grün“ quittiert.

Ist der persönliche Kontakt nicht möglich, kann der öffentliche Schlüssel auch vom Server des Betreibers heruntergeladen werden. Zuvor verifiziert der Server per SMS oder E-Mail, dass der öffentliche Schlüssel tatsächlich der Person gehört, als die sie sich ausgibt.

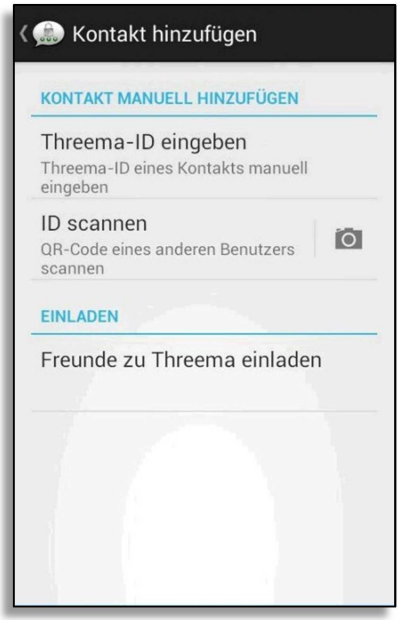


Abb. 25: Kontakt hinzufügen

190 Threema ermöglicht auch beliebige Dateien bis zu 20 Mbyte Größe verschlüsselt an Chat-Partner zu versenden. Webseite des Entwicklers: https://threema.ch/de
191 http://hoccer.com/de/

Die Personalien des Nachrichtenempfängers werden hierbei nicht überprüft. Die Sicherheitsstufe wird mit „orange“ angezeigt. Deine persönliche Threema-ID und dein QR-Code sowie den Fingerprint des öffentlichen Schlüssels findest du unter dem Informationssymbol oben rechts im Bildschirm. Du kannst bei Bedarf die Threema-ID auch löschen lassen, etwa dann wenn dir dein Handy gestohlen wurde. Zuvor musst du in der App ein spezielles Widerrufspasswort über das Menü-Symbol oben links und *ID-Widerruf* festlegen. Gibst du deine Nutzer-ID und das Widerrufspasswort auf einer eigenen Threema-Webseite[192] ein, werden deine Nutzer-ID und alle weiteren damit verbundenen Informationen unwiderruflich gelöscht.

Einen sicheren Austausch von Chat-Nachrichten bietet auch Hoccer.[193] Die App lässt sich ohne Angabe von Name, Telefonnummer oder E-Mail-Adresse nutzen, zur Anmeldung reicht ein Nickname. Zudem geht die App sparsam mit den persönlichen Daten der Nutzer um. Hoccer greift nicht auf das Telefonbuch zu, neue Kontakte müssen manuell per Einladung über SMS, E-Mail oder QR-Code hinzugefügt werden. Auch Vertraulichkeit ist gewährleistet, die Nachrichten und Dateien sind immer Ende-zu-Ende verschlüsselt, sodass nur Sender und Empfänger sie lesen können.

Größten Wert auf den Schutz der Privatsphäre legt auch die Open-Source-App ChatSecure.[194] Mit der Crypto-App kann der Chat auch über das Anonymisierungsnetzwerk Tor geleitet werden.

4.6.2.2 Cloud verschlüsseln

Viele Menschen nutzen Speicherplatz im Web, um ihre Fotos und Videos zu teilen, gemeinsam an einem Vortrag zu arbeiten, ihre Dokumente im Web zu sichern und auch um unterwegs darauf zugreifen zu können. Die Achillesferse vieler Cloud-Dienste ist, dass sich die Anwender nie sicher sein können, dass die eigenen Daten wirksam vor Cyberkriminellen und Diensten[195] geschützt sind. Damit Angriffe auf die Cloud-Daten ins Leere laufen, müssen die Daten bereits vor der Übertragung in die Datenwolke auf dem PC oder Smartphone des Nutzers verschlüsselt werden.

Wer seine Daten in der Cloud speichern möchte, aber vor dem Hintergrund der NSA-Spähaffäre vorsichtig geworden ist, findet auch europäische Alternativen zu Dropbox & Co. Zum Schutz der eigenen Daten sollte der

192 https://myid.threema.ch/revoke
193 Webseite des Entwicklers: http://hoccer.com/de/
194 ChatSecure ist Teil des The Guardian Project, das sich den Schutz der digitalen Privatsphäre auf die Fahnen geschrieben hat: https://guardianproject.info/
195 Mit den geheimen National Security Letters kann das FBI Cloud-Anbieter, die ihren Sitz in den USA haben, zur Preisgabe von Cloud-Daten zwingen. Der Bürger erfährt davon nichts. Damit der Datenzugriff geheim bleibt, wird der betroffene Cloud-Dienst verpflichtet, zu schweigen.

Cloud-Dienstleister eine Ende-zu-Ende-Verschlüsselung anbieten. Nur Personen, die das Passwort kennen, können dann die Daten entschlüsseln.

Anbieter (Sitz)	Webadresse	Speicherplatz in GB (kostenlos)	Betriebssysteme
Google Drive (USA)	https://drive.google.com	15 GB	Win, Mac, iOS, Android, Linux
Dropbox (USA)	https://www.dropbox.com	2 GB	Win, Mac, iOS, Android, Linux
SpiderOak[196] (USA)	https://spideroak.com	2 GB	Win, Mac, iOS, Android, Linux
Strato HiDrive (BRD)	https://www.free-hidrive.com	5 GB	Win, Mac, iOS, Android, Linux
TeamDrive[197] (BRD)	https://www.teamdrive.com/de	2 GB	Win, Mac, iOS, Android, Linux
Tresorit[198] (Schweiz)	https://tresorit.com	3 GB	Win, iOS, Android, Windows Phone

Tab. 13: Cloud-Anbieter

Manuelles Verschlüsseln

Einige Speicher-Dienste wie Dropbox bieten nur eine Verschlüsselung des Transportweges an. Anwender können jedoch die Sicherheit ihrer privaten Daten verbessern, indem sie diese bereits lokal verschlüsseln. Dafür gibt es Tools für PCs und Smartphones.

Mit VeraCrypt[199] beispielsweise kannst du auf PCs verschlüsselte Ordner erstellen. In den Datentresor verschiebst du deine vertraulichen Daten und speicherst den gesamten Datentresor in deiner Cloud ab. Kommen in den Datentresor neue Daten hinzu, gleichst du deinen lokalen Container mit dem Cloud-Container ab. Deine Daten sind somit verschlüsselt, bevor sie in die Cloud hochgeladen werden. Auf dem Handy kannst du mithilfe der App EDS[200] Datentresore anlegen und mit der Cloud synchronisieren. EDS kann auch die VeraCrypt-Archive einlesen. Das ermöglicht dir, den Datentresor zunächst einfacher auf dem PC zu erstellen, vertrauliche Daten in den Datentresor zu verfrachten und diesen darauf mithilfe eines USB-Kabels und einem Sync-Tool aufs Handy zu kopieren. Auf dem Handy bindest du das VeraCrypt-Archiv in die EDS-App ein.

196 Mit Ende-zu-Ende-Verschlüsselung.
197 Mit Ende-zu-Ende-Verschlüsselung.
198 Mit Ende-zu-Ende-Verschlüsselung.
199 Produktwebseite: https://veracrypt.codeplex.com/; VeraCrypt ist eine quelloffene Software, die somit jederzeit von IT-Experten auf Sicherheitslücken überprüft werden kann. Tutorial: https://veracrypt.codeplex.com/wikipage?title=Beginner%27s%20Tutorial
200 Die EDS-App wird in Google Play angeboten.

Die manuelle Verschlüsselung ist geeignet, wenn du die Cloud nur dafür nutzt, um deine Daten zu sichern und um auch unterwegs darauf zugreifen zu können. Manuelle Lösungen sind ungeeignet, will man die eigenen Daten über die Cloud auch mit anderen Personen teilen.

Cloud per App verschlüsseln

Bequemer sind Tools wie TeamDrive,[201] mit dem du Daten verschlüsselt übers Netz tauschen und von jedem PC oder Smartphone darauf zugreifen kannst. Zentraler Sicherheitsaspekt von TeamDrive ist eine Ende-zu-Ende-Verschlüsselung. Um den Cloud-Service nutzen zu können, musst du dich während der Installation beim Anbieter registrieren. Nur registrierten Nutzern kannst du später den Zugriff auf deine Cloud-Daten ermöglichen. Wie geht's?

Installation und Registrierung: Lade TeamDrive aus dem Play Store und installiere die App. Nach der Installation musst du dich zunächst beim Cloud-Dienst registrieren. Lege dazu Benutzername und Passwort[202] fest, gib eine gültige E-Mail-Adresse ein, akzeptiere die Lizenzbedingungen und bestätige mit *Registrieren*. Anschließend erhältst du eine E-Mail mit einem Aktivierungslink, den du bestätigen musst, damit das neu erstellte Konto freigeschaltet wird. Für den privaten Gebrauch ist die App kostenlos.

Cloud-Dienste: technische Fragen

- Welche Betriebssysteme unterstützt der Cloud-Dienst: Windows, Mac, Linux, iOS oder Android?
- Sind die Transportwege der Daten verschlüsselt?
- Werden die gesendeten Inhalte verschlüsselt (Ende-zu-Ende-Verschlüsselung)?
- Entstehen bei der Nutzung Metadaten, über die der Cloud-Betreiber sieht, wer mit wem wann über welche Dienste kommuniziert hat?
- Handelt es sich bei den Crytpo-Tools um quelloffene Programme, die jederzeit von jedem eingesehen und überprüft werden können?

Ordner und Dateien verwalten: Die Hauptfunktion von TeamDrive ist der Austausch von Daten zwischen PCs, Tablets oder Smartphones. Den Datenabgleich aller Dateien und Ordner führt TeamDrive über sogenannte Spaces durch. Nach der Installation der App musst du dir zunächst einen solchen Speicherbereich einrichten. Dies ist schnell über das Seitenmenü erledigt. Tippe hierfür auf *Space erstellen*, benenne den neuen Space und bestätige mit *Space erstellen*. Der Name des neu angelegten Space erscheint nun auf allen PCs, Tablets und Smartphones, mit denen du später Daten austauschst.

Um Fotos teilen zu können, musst du diese zuvor im lokalen Space speichern. Öffne hierfür den Space, in den du die Fotos importieren möchtest. Tippe danach auf das Import-Symbol und navigiere als Nächstes über *Importiere vom Foto-Album* zum Speicherort der Fotos. Nun wählst du die gewünschten Fotos aus und tippst

201 https://www.teamdrive.com/de

202 Ein sicheres Passwort sollte mindesten 16 Zeichen lang sein, Groß-, Kleinbuchstaben, Zahlen und Sonderzeichen enthalten, aber unter TeamDrive keine Leerzeichen. Keepass2Android ist ein Passwortmanager, mit dem du einfach sichere Passwörter erstellen und verwalten kannst.

auf *Weiter*. Die im Space abgelegten Fotos werden sodann automatisch mit der Cloud synchronisiert. Andere Dateitypen, wie Word-Dateien, können (vorerst) nur auf dem PC per Drag and Drop dem Space hinzugefügt werden. Um Word-Dateien aufs Handy zu bekommen, müssen sie also auf dem PC ins Space-Verzeichnis kopiert und über die Cloud an die App geschickt werden.

Dateien teilen: Willst du deinen Freunden den Zugriff auf deinen Cloud-Speicher erlauben, musst du sie zuvor dazu einladen. Wähle zunächst den Space aus, den du für deine Freunde freigeben willst. Ein Swipe von rechts nach links zeigt ein Untermenü mit der Funktion *Benutzer hinzufügen* an. Tippe darauf und du bist bei den Einladungsoptionen. Um Mitglieder einzuladen, musst du ihre E-Mail-Adresse eingeben. Die Einladung kannst du eventuell mit einem Passwort schützen. Das Passwort bietet mehr Sicherheit; Eingeladene können dann nur mit Eingabe des Passwortes dem Space beitreten. Füge nun den Eingeladenen über das Pluszeichen der Einladungsliste hinzu. Tippe abschließend auf *Einladen* und der eingeladene Freund erhält darauf einen entsprechenden Hinweis sowohl per E-Mail als auch in TeamDrive unter *Einladungen*. Wird die Einladung akzeptiert, erscheint unter *Aktive Space* der Name des neu verknüpften Space mit deinem Benutzernamen. Die Dateien, die du in den geteilten Space kopierst, werden dann automatisch auf das damit verknüpfte Smartphone übertragen. Freunde, mit denen du einen Space teilst, können die eingeräumten Nutzungsrechte jedoch nicht ihrerseits an ihre Freunde übertragen. Damit behältst du die Kontrolle über die Zugriffsrechte zu deinem Online-Speicher. Die eingebaute Versionsverwaltung stellt sicher, dass jede Änderung an Inhalten automatisch erfasst wird und ermöglicht dadurch, dass alle Mitglieder eines Spaces diese auch nachvollziehen können. Teams können so gemeinsam an Dokumenten arbeiten.

Cloud-Dienste: rechtliche Fragen

- Welchem nationalen Recht unterliegt der Datenschutz der Cloud-Server?
- Ist für die Datenabfrage eine richterliche Anordnung erforderlich?
- In welchen Fällen darf eine Datenabfrage angeordnet werden? Reicht dazu ein bloßer Verdacht aus? Ist sie nur auf schwere Straftaten begrenzt?
- Bietet der Cloud-Dienst ein „Verfahrensverzeichnis“, in dem transparent geregelt wird, wie der Dienst mit den Nutzerdaten umgeht und an wen sie weitergeleitet werden?

Lokale Daten schützen: So wie bekanntlich die Stärke einer Kette vom schwächsten Glied abhängt, hängt die Sicherheit deiner privaten Daten auf dem Handy davon ab, wie gut du sie vor unerlaubtem Zugriff schützt. Zum minimalen Schutz gehört, die SIM-PIN zu aktivieren sowie die Bildschirmsperre zu nutzen. Effektiven Schutz erzielst du aber nur, wenn du dein Smartphone komplett verschlüsselst.

„Private Cloud“ verschlüsseln

Nutzer, die ihre Daten nicht Servern in der Cloud anvertrauen wollen, können auch eine „private Cloud“ einrichten.[203] Mit der Freeware BitTorrent Sync[204] beispielsweise kannst du Dateien zwischen beliebig vielen PCs, Notebooks oder Smartphones synchronisieren - ein zentraler Server ist nicht erforderlich. Deine Daten werden nur an die von dir autorisierten Endgeräte gesendet. Der Datenabgleich erfolgt über eine Ende-zu-Ende-Verschlüsselung.

Abb. 26: Berechtigung per QR-Code weitergeben

Installation und Einrichtung: Lade die BitTorrent-App[205] aus dem Play-Store herunter und installiere sie. Willst du dein Smartphone mit deinem PC verbinden, auf dem bereits BitTorrent installiert ist, dann tippe auf *Ein Gerät verknüpfen, auf dem bereits Sync 2.0 läuft*. Der Schlüsselaustausch zwischen Handy und PC kann über einen QR-Code erfolgen. Starte dazu auf deinem PC das Sync-Tool, klicke auf das Zahnrad oben rechts und wähle *Meine Geräte…* Im nächsten Fenster drückst du auf *Gerät verknüpfen* und es wird dir ein QR-Code angezeigt. Diesen kannst du nun mit dem Smartphone vom Bildschirm des PCs abfotografieren und Handy und PC sind miteinander verknüpft. Die Sync-Ordner, die du bereits auf dem PC angelegt hast, erscheinen darauf als Vorschau auf dem Handy. Willst du die Sync-Ordner deines Rechners der Sync-App hinzufügen, musst du auf den Sync-Ordner tippen und dies mit *OK* bestätigen. Das Sync-Ordner-Symbol verwandelt sich daraufhin in eine Krone.

Bevor du beginnst Daten zu teilen, solltest du dir überlegen, wo du den Sync-Ordner speichern willst. Unter *Menü/Einstellungen/Erweitert/Standardspeicherort* kannst du den Speicherort ändern. Werden vertrauliche Daten synchronisiert, sollte der Sync-Ordner in einen verschlüsselten Datentresor[206] verschoben werden.

Dateien teilen: Personen, mit denen du Fotos, Videos oder Dokumente teilen willst, erhalten die Daten erst, wenn du ihnen dafür die entsprechende Berechtigung einräumst. Dafür wird ein sogenanntes „Secret“ erstellt. Dabei handelt es sich um eine Kombination aus Zahlen und Buchstaben. Auf berechtigten Endgeräten muss nur dieses Secret eingegeben werden und die Daten des Sync-Ordners werden synchronisiert.

203 Für technisch versierte Nutzer etwa mit der freien und kostenlosen Cloud-Software ownCloud: http://owncloud.org/; Tutorial: http://www.web266.de/tutorials/cloud-online-speicher/owncloud.html. Oliver Diedrich u. a. (2011): *Herr der eigenen Daten. Private Infrastruktur für digitale Nomaden,* c’t 2011, Heft 15, S. 130-132.
204 Webseite des Entwicklers: https://www.getsync.com/; in der kostenlosen Version dürfen maximal 10 Ordner abgeglichen werden.
205 https://www.getsync.com/intl/de/platforms/desktop. In der kostenlosen Free-Version steht BitTorrent für Windows, Mac OS X, Linux und FreeBSD zur Verfügung; Apps gibt es für Android, iOS und Windows Phone.
206 Verschlüsselte Datentresore kannst du mithilfe der EDS-App erstellen.

Wie geht’s? Gehe zum Sync-Ordner, den du teilen möchtest, tippe rechts auf die Menü-Punkte und wähle im geöffneten Menü *Verteilen.* Lege die Zugriffsrechte fest und bestimme, ob diese per E-Mail, per Kopieren oder per QR-Code weitergegeben werden sollen. Triffst du die Person, mit der du Inhalte teilen willst, dann scannt diese am besten den QR-Code mit der mobilen App Sync, um die gewährten Zugriffsrechte auf deinen Sync-Ordner zu erhalten.

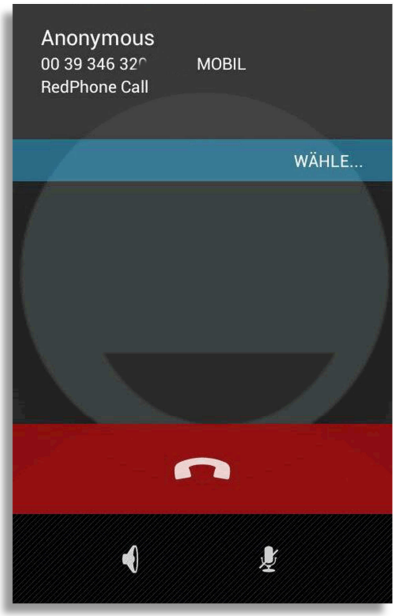


Abb. 27: Verschlüsselt telefonieren

4.6.2.3 Telefonat verschlüsseln

Nicht jedes Telefonat ist für die Öffentlichkeit bestimmt, etwa wenn Geschäftspartner oder Techniker sensible Informationen austauschen. Fängt die Konkurrenz die Gespräche ab, kann das für das Pionierunternehmen verheerende ökonomische Folgen haben. RedPhone[207] ist eine VoIP-Telefonie-App für Android-Handys. Telefonate werden dabei verschlüsselt über das Internet geführt - entweder über eine 3G- oder WLAN-Verbindung. Die Telefonie-App ist Open-Source und steht unter der GNU General Public License (GPL). Das bedeutet, jeder Interessierte kann den Quellcode herunterladen und ihn auf Sicherheitslücken oder eventuelle Hintertüren für „Lauscher“ analysieren. RedPhone-Gespräche sind nur zwischen registrierten Rufnummern möglich.

So geht’s: Zunächst musst du dich bei RedPhone mit deinem Land, der Landesvorwahl und deiner Telefonnummer registrieren. Kurz darauf erhältst du zur Verifizierung deiner Telefonnummer eine Bestätigungs-SMS. Du kannst nun mit allen Personen abhörsicher telefonieren, die auch RedPhone auf ihrem Handy installiert haben. Beim Telefonieren über RedPhone musst du dich nicht anmelden oder einloggen. RedPhone nutzt die registrierten Telefonnummern und wählt diese an. Ruft dich ein RedPhone-Teilnehmer an, ertönt dein normaler Klingelton. Außer an der kurzen Verzögerung bei der Gesprächsaufnahme merkst du keinen Unterschied zum normalen Telefonat.

4.6.2.4 E-Mails verschlüsseln

Gefahren: E-Mails werden im Internet im Klartext übertragen; sie können also nach Belieben von Cyberkriminellen oder auch von Behörden gelesen werden. Zudem besteht die Gefahr, dass Absender und Inhalt von Betrügern auf dem Weg zum E-Mail-Empfänger manipuliert werden können. Das Grundrecht eines jeden Menschen auf „geheimen Schriftverkehr“ (Art. 15 Verf.) ist im Netz nicht automatisch gewährleistet.

207 RedPhone wird in Google Play angeboten; Entwickler-Webseite: https://whispersystems.org/

Sicherheitsmaßnahmen: Als Schutzmaßnahmen können die E-Mail-Transportwege abgesichert und/oder die E-Mail-Inhalte verschlüsselt werden.

Erstens, wähle für deinen E-Mail-Verkehr einen sicheren und vertrauenswürdigen E-Mail-Dienst.[208] Auf dem Weg vom Absender zum Empfänger der E-Mails passiert eine Nachricht viele Server. Kriminelle oder Dienste können die Nachrichten abfangen und mitlesen. Die Angriffsform wird als „man-in-the-middle-attack“ bezeichnet. Eine Abwehrmaßnahme besteht darin, den Transportweg vom Absender und Empfänger der E-Mails zu den Servern der Mail-Dienste zu verschlüsseln.[209] Der „Mann in der Mitte“ kann die E-Mail-Nachricht nicht mehr so ohne weiteres mitlesen. Bei der Wahl des Maildienstes ist zu bedenken, dass für alle US-Unternehmen der „Patriot Act“[210] gilt, der sie dazu verpflichtet, alle Kundendaten und E-Mails an die US-Behörden herauszugeben – unabhängig davon, in welchem Land der Server steht. Zweitens, wirklichen Schutz vor Datenspionage bieten nur verschlüsselte E-Mail-Inhalte.

Checkliste: Sichere Mail-Dienste

- Ermöglicht der Mail-Anbieter eine Verschlüsselung des Transportweges?
- Gibt es eine optionale Eingangs-Verschlüsselung des Postfachs beim Mail-Dienst?
- Kann das E-Mail-Konto anonym eingerichtet und anonym bezahlt werden?
- Scannen die E-Mail-Dienste ein- und ausgehende Mails ihrer Kunden, um zielgenau Werbung zu schalten?
- Werden die Kundendaten und E-Mails auf Servern in einem EU-Staat gespeichert?

Das Public-Key-Verfahren

Wie funktioniert die E-Mail-Verschlüsselung? Anwendung findet dabei das sog. Public-Key-Verfahren. Dieses Verfahren arbeitet mit einem Schlüsselpaar: der öffentliche Schlüssel dient dazu, die E-Mail-Nachricht an den Empfänger zu verschlüsseln. Der Empfänger der verschlüsselten Nachricht entschlüsselt sie mit seinem (geheimen) privaten Schlüssel. Für E-Mail-Verschlüsselung gibt es bis heute zwei Standards: S/MIME und OpenPGP.[211]

---

208 Nach Stiftung Warentest (12.02.2015) bieten die Maildienste Posteo (https://posteo.de) und Mailbox.org (https://mailbox.org) den besten Schutz von Kundendaten und E-Mails: https://www.test.de/E-Mail-Provider-im-Test-Nur-einer-liest-nicht-mit-4806144-0/

209 Aktiviere hierfür die SSL-Verschlüsselung bei Mozilla Thunderbird. Starte Thunderbird und öffne über den Menüpunkt *Extra/Konten-Einstellungen* die Kontenkonfiguration. Klicke auf der linken Seite auf *Server-Einstellungen*. Wähle unter dem Punkt *Verbindungssicherheit* SSL/TLS. Handelt es sich um den Servertyp IMAP, dann wähle Port 993, beim Servertyp POP3 den Port 995. Wechsle nun zum Punkt *Postausgangs-Server (SMTP)* und drücke auf *Bearbeiten…* Im nächsten Pop-up-Fenster stelle unter *Verbindungssicherheit* entweder auf STARTTLS oder SSL/TLS. Bestätige per Klick auf *OK* und danach die Konten-Einstellungen ebenfalls per Klick auf *Ok*. Haben Absender und Empfänger der E-Mail das Mail-Konto bei demselben Maildienst, ist eine lückenlose Verschlüsselung des Transportweges sichergestellt. Ist das nicht der Fall, kann u. U. der Transportweg zwischen den Mailservern ungesichert erfolgen.

210 „USA PATRIOT Act“. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 3. Juni 2015, 11:55 UTC. URL: http://de.wikipedia.org/w/index.php?title=USA_PATRIOT_Act&oldid=142724104 (Abgerufen: 11. Juni 2015, 16:35 UTC)

211 Das „Gpg4win-Kompendium“ liefert einen Überblick für „Einsteiger“ und „Durchblicker“ über die Funktionsweise der E-Mail-Verschlüsselung: http://www.gpg4win.de/documentation-de.html

Der S/MIME-Standard setzt auf Zertifizierungsstellen (Certification Authority, kurz CA). Eine sichere Authentifizierung des Absenders muss gewährleisten, dass ein bestimmter öffentlicher Schlüssel eindeutig einer bestimmten Person zuzuordnen ist. Für die Authentizität stehen die Zertifizierungsstellen ein. Sie überprüfen die Identität des Antragstellers und bestätigen diese mit ihrer Signatur.

Tipp

Sichere dein Schlüsselpaar auf einem externen Datenträger (SD-Karte, USB-Stick). Sollte dein Handy einmal verloren gehen, kannst du das gesicherte Schlüsselpaar in den APG-Schlüsselring auf deinem neuen Handy importieren.

Der OpenPGP-Standard beruht auf einem „Netzwerk des Vertrauens". Die Beglaubigung des öffentlichen Schlüssels erfolgt durch die Teilnehmer der E-Mail-Nachrichten. Gregor, der eine signierte und verschlüsselte E-Mail von Eva erhält, vertraut darauf, dass Eva wirklich Eva ist, weil ihr öffentlicher Schlüssel von Alice und Greta unterschrieben wurde; beide sind für Gregor vertrauenswürdige Personen. Zur Verschlüsselung der E-Mails benötigst du lediglich die Apps K-9 Mail und OpenKeychain.

Mit OpenKeychain[212] E-Mails verschlüsseln

OpenKeychain ist eine Krypto-App, mit der du E-Mails und Dateien verschlüsseln und signieren kannst. Installiere zunächst die Krypto-App. Bevor du aber abhörsicher E-Mail-Nachrichten austauschen kannst, musst du ein Schlüsselpaar erstellen. Öffne die App und tippe zunächst auf *Menü/Einstellungen/Fortgeschrittene Einstellungen*. Ändere im nächsten Fenster den voreingestellten Hashalgorithmus auf den Wert SHA-512. Gehe nun zurück zum Hauptfenster und tippe anschließend auf *Menü/Erzeuge meinen Schlüssel*. Vergib auf der nächsten Seite einen Nutzernamen, trage die E-Mail-Adresse ein, wähle ein sicheres Passwort und tippe auf *Weiter*. Mit *Schlüssel erzeugen* erstellt die App ein neues Schlüsselpaar. Ist die Erstellung abgeschlossen, wird dir unter *Meine Schlüssel* die E-Mail-Adresse angezeigt, mit der das neue Schlüsselpaar verknüpft ist. Tippe auf die E-Mail-Adresse und dann auf *Teilen*, darauf werden dir die Schlüssel-ID, der Fingerabdruck und der entsprechende QR-Code angezeigt. Besitzt du bereits ein Schlüsselpaar,[213] mit dem du mit Enigmail für Thunderbird verschlüsselst, kannst du dieses auch über *Menü/Datei importieren* in den Schlüsselring importieren.[214]

Um verschlüsselte E-Mails versenden zu können, benötigst du den öffentlichen Schlüssel des E-Mail-Empfängers. Diesen kannst du per E-Mail-Anhang beziehen, von einer Webseite oder von einem öffentlichen

212 OpenKeychain wird in Google Play angeboten; Entwickler-Webseite: http://www.openkeychain.org/

213 Anleitungen zur E-Mail-Verschlüsselung mit GnuPG für Windows findest du hier: http://www.german-privacy-fund.de/e-mails-verschlusseln-leicht-gemacht/; http://www.gpg4win.de/doc/de/gpg4win-compendium.html

214 Dein Schlüsselpaar musst du in Mozilla Thunderbird aus deinem OpenPGP-Schlüsselbund exportieren. Öffne hierfür die OpenPGP-Schlüsselverwaltung, wähle dein Schlüsselpaar aus, klicke auf *Datei/Exportieren* und im nächsten Dialog auf *Geheime Schlüssel exportieren*. Als Zielverzeichnis wählst du deine microSD-Karte aus.

Schlüsselserver herunterladen. Das Risiko bei PGP-Schlüsseln ist, „gefälschten Schlüsseln“ auf den Leim zu gehen. Jeder kann sich einen Schlüssel auf einen beliebigen Namen und eine beliebige E-Mail-Adresse ausstellen und auf Schlüsselserver oder Webseiten hochladen. Es führt kein Weg daran vorbei, den öffentlichen Schlüssel mithilfe des Fingerabdrucks zu überprüfen. Der Fingerabdruck ist weltweit eindeutig, er besteht aus einer Folge von zehn Blöcken, die jeweils aus vier Zeichen bestehen. Haben Absender und Empfänger denselben Fingerabdruck, dann besitzen sie auch denselben Schlüssel. Den Fingerabdruck kannst du per Telefon abgleichen. Dein Gegenüber liest dir dazu beispielsweise den ersten, den fünften und zehnten Ziffernblock vor. Willst du höchste Sicherheit, dann triff dich persönlich mit dem Schlüsselinhaber und verifiziere den Fingerabdruck vor Ort oder fotografiere den entsprechenden QR-Code direkt vom Handy ab. Hast du den Schlüssel überprüft, kannst du ihn signieren und verwenden.[215]

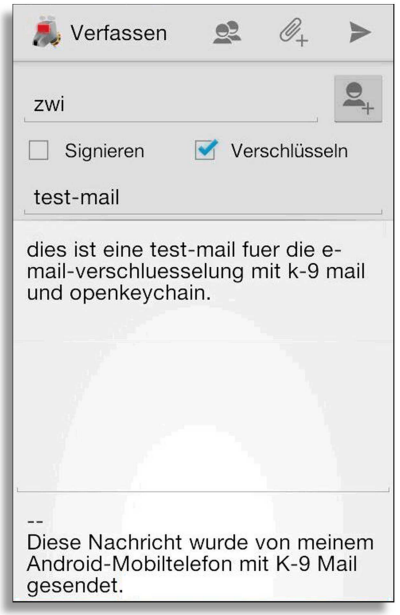


Abb. 28: E-Mail-Verschlüsselung

Mit K-9 Mail[216] E-Mails senden und empfangen

K-9 Mail ist eine Open-Source-App, die OpenKeychain unterstützt. So kannst du beim Versenden einer Mail wählen, ob die Nachricht nur verschlüsselt, nur signiert oder verschlüsselt und signiert werden soll.

Zunächst musst du dein E-Mail-Konto einrichten. Öffne die App und gib E-Mail-Adresse und Passwort ein. Das sind die Zugangsdaten für die eintreffenden E-Mails. Tippe auf *Weiter* und wähle auf der folgenden Seite *POP3-Konto* aus. Bei den Einstellungen für den Posteingangsserver trägst du die E-Mail-Adresse als Benutzername ein und gib den POP3-Server deines E-Mail-Anbieters (Providers) an. Stelle den Sicherheitstyp auf *SSL/TLS* – so ist der Transportweg vom E-Mail-Server zum E-Mail-Programm gesichert. Tippe auf *Weiter*. Hast du alles korrekt eingegeben, kannst du auf der nächsten Seite sogleich auf *Weiter* tippen. Auf der abschließenden Seite trägst du noch einen Kontonamen und deinen Namen dein, der für alle E-Mail-Empfänger sichtbar ist. Nun musst du noch die Einstellungen für den Postausgangsserver vornehmen. Gib den SMTP-Server deines E-Mail-Anbieter an und stelle den Sicherheitstyp auf SSL/TLS – so ist der Versandweg zum E-Mail-Server verschlüsselt. Auf der nächsten Seite musst du noch einen Kontonamen und deinen Namen eintragen, der für alle E-Mail-Empfänger sichtbar ist. Mit *Fertig* ist die Ein-

215 Zusätzlich kannst du noch das Besitzer-Vertrauen festlegen. Damit zeigst du an, wie sehr du dem E-Mail-Empfänger zutraust, öffentliche Schlüssel anderer sorgfältig zu verifizieren. Das Besitzer-Vertrauen ist für die verschlüsselte E-Mail-Kommunikation selbst unwichtig. Relevant ist es, wenn du von einer Person einen öffentlichen Schlüssel erhältst und dieser bereits von einer Person unterschrieben ist, der du „absolut“ das Besitzer-Vertrauen ausgesprochen hast. Du kannst dir dann ersparen, den Fingerabdruck zu überprüfen, weil dies bereits eine vertrauenswürdige Person/Stelle erledigt hat.

216 K-9 Mail wird in Google Play angeboten; Entwickler-Webseite: https://code.google.com/p/k9mail/

richtung abgeschlossen. Die OpenKeychain-Unterstützung muss in K-9 Mail noch aktiviert werden. Du findest diese unter *Menü/Einstellungen/Kryptographie* auf *OpenPGP-Provider.* Wähle hier deine Schlüsselverwaltung *OpenKeychain.*[217] Nun ist alles vorbereitet, um die erste E-Mail zu verschlüsseln oder zu signieren.

E-Mails verschlüsseln und signieren

Verfasse wie üblich eine E-Mail-Nachricht. Oberhalb der Betreffzeile werden zwei Optionen angezeigt, mit denen du die aktuelle Nachricht verschlüsseln oder unterzeichnen kannst. Aktivierst du auch *Signieren*, musst du vor dem Senden das Passwort deines privaten Schlüssels eingeben. Nun ist alles fertig, um die Nachricht abhörsicher mit einem Tipp auf das Senden-Symbol abzuschicken. Erhältst du eine Nachricht, die mit deinem öffentlichen OpenPGP-Schlüssel verschlüsselt ist, dann musst du zuvor dein Passwort eingeben, damit die Nachricht im Klartest angezeigt wird.[218]

4.6.3 Passwortmanager

Gefahren: Bei der Nutzung vieler Internetdienste sind Passwörter unerlässlich. Man benötigt sie für E-Mail-Konten, Foren, eShops, eBay, soziale Netzwerke oder verschlüsselte Containerdateien. Mit einem Passwort weist sich eine Person aus, dass sie zum Zugriff auf geschützte Daten berechtigt ist. Das Problem ist, dass sich im Laufe der Zeit immer mehr Passwörter ansammeln und sich niemand alle sicheren Passwörter merken kann. Unsichere Passwörter, wie „111“, „passwort“ oder 0471123456“ sind für Betrüger geradezu eine Einladung, in deinem Namen bei eShops zu bestellen, E-Mails zu versenden oder mal nachzusehen, was sich hinter deiner verschlüsselten Containerdatei alles verbirgt. Zum Schutz deiner digitalen Privatsphäre sind sichere Passwörter unentbehrlich.

Checkliste: Passwortmanager

- Werden aktuelle Verschlüsselungsstandards zur Verschlüsselung der Datenbank eingesetzt?
- Hat die App auch einen Passwortgenerator an Bord?
- Ist die Oberfläche klar aufgebaut und kann sie intuitiv bedient werden? Kann man die Passwörter nach Bereichen ordnen, wie Homebanking, eMail, Internet?
- Übermittelt die App ungefragt Systemdaten, Nutzungsstatistiken oder Absturzberichte an den Anbieter?
- Sind in der Vergangenheit gravierende Sicherheitslücken bekannt geworden?
- Handelt es sich um eine App, die von renommierten Sicherheitsfirmen oder Instituten zertifiziert wurde?
- Handelt es sich um eine freie (GPL-Lizenz) oder proprietäre Software (klassisches Urheberrecht)?
- Gibt es eine Hilfe-Funktion, ein Benutzerhandbuch, ein Forum oder einen Support?

217 Die Option einer S/MIME-Verschlüsselung ist nicht vorgesehen.

218 Verschlüsselte E-Mails sichern Vertraulichkeit aber nicht Anonymität. Die Metadaten der E-Mails, also Empfänger, Absender, Versandzeit und Betreff sind weiterhin lesbar. Über die Metadaten lässt sich feststellen, wer mit wem, wie oft und wann E-Mails ausgetauscht hat. Versendet der Nutzer die E-Mails per Smartphone, kommen noch die SIM-Kartennummer, die Gerätenummer des Handys und die Standortdaten hinzu.

Sicherheitsmaßnahme: Inzwischen gibt es eine Reihe von Passwort-Managern, mit denen du bequem sichere Passwörter generieren und verwalten kannst. Keepass2Android[219] ist eine kostenlose App für Android. Die App benutzt das Datenbank-Format des KeePass2.x-Passwortmanagers[220] für Windows und andere Betriebssysteme. Du kannst also die Passwortdatenbank, die du zuvor am PC verwendet hast, auch am Smartphone nutzen. All deine Passwörter werden in einer verschlüsselten Datenbank (AES 256-Bit-Schlüssel) gespeichert. Fortan musst du nur noch das Zugangs-Passwort eintippen und kannst auf deine hinterlegten Passwörter zugreifen.[221]

Abb. 29: Passwort-Generator

KeePass2Android-Datenbank erstellen

Installiere zunächst über Google Play Keepass2Android auf deinem Handy. Erstelle als Erstes eine neue Datenbank. Tippe hierzu nach dem Start der App auf *Neue Datenbank erstellen…*. Wähle nun Speicherort und Dateiname der Datenbank aus. Aus Sicherheitsgründen solltest du als Datenträger einen USB-Stick mit microUSB-Anschluss wählen. Benötigst du den Passwortmanager nicht mehr, ziehst du den USB-Stick vorsichtshalber vom Handy ab. Tippe auf *Erstellen*, dann wirst du zur Eingabe des Hauptschlüssels weitergeleitet. Du hast die Wahl zwischen einem Kennwort[222] und einer Schlüsseldatei.[223] Das Kennwort sollte eine Mindestlänge von 16 Zeichen haben und Groß-, Kleinbuchstaben, Zahlen und Sonderzeichen aufweisen. Nach der Eingabe des Hauptschlüssels wird die Datenbank erstellt und der Passwortmanager ist schon betriebsbereit. Willst du später den Hauptschlüssel ändern, dann tippe im Hauptfenster auf die Menü-Taste und dann auf den Eintrag *Datenbank-Kennwort ändern*.

Passwörter verwalten

Öffne KeePass2Android und du wirst als Erstes aufgefordert, das Kennwort und/oder die Schlüsseldatei zum Entschlüsseln der Datenbank einzugeben. Du kannst hier auch ein Häkchen vor *Als Standard-Datenbank benut-*

219 KeePass2Android wird in Google Play angeboten.
220 http://keepass.info
221 Eine Alternative zu den Passwort-Managern bildet das Master-Passwort-Verfahren. Der Anwender merkt sich dabei auch nur ein einziges sicheres Passwort. Für jeden Dienst wird dann ein eigenes Passwort erzeugt, das aus der Kombination von Master-Passwort und Dienst hervorgeht. Der Vorteil dieses Verfahrens ist, dass keine Passwörter gespeichert, sondern nur bei Bedarf neu berechnet werden. Die Open-Source-App Master Password (http://masterpasswordapp.com/) wendet beispielsweise das Master-Passwort-Verfahren an.
222 Für das Zugangs-Passwort kannst du auch eine sogenannte Passwortkarte verwenden: http://www.savernova.com/de/sichere-passworter/
223 Eine Schlüsseldatei kannst du beispielsweise mit dem Tool TrueCrypt (Extras/Schlüsseldatei erstellen…) erstellen. Speichere die Schlüsseldatei auf einen USB-Stick mit micro-USB-Anschluss und verwende diesen zur Sicherheit nur für die Schlüsseldatei.

zen setzen, falls du für das Handy nur eine einzige Datenbankdatei verwendest. Bestätige die Eingabe mit *OK* und du gelangst zum Hauptfenster der App. Hier kannst du Accounts eintragen, bearbeiten und löschen. Die Accounts sind in Gruppen unterteilt. Willst du eine neue Gruppe hinzufügen, etwa für Homebanking, dann tippe einfach unten links auf *GRUPPE HINZUFÜGEN*, gib den Namen für die Gruppe ein und bestätige mit *OK*.

Willst du einen Eintrag zur eMail-Gruppe für dein Web-Mail hinzufügen, dann tippe auf die Gruppe *eMail* und unten rechts im Bildschirm auf *EINTRAG HINZUFÜGEN*. Im nächsten Fenster gibst du die Eigenschaften des neuen Eintrags ein. Wähle einen passenden Titel, etwa den Namen des Anbieters der Web-Mail, Benutzername und das Kennwort. Hast du noch kein Kennwort für dein Web-Mail und willst du ein sicheres erzeugen, dann tippe rechts vom Kennwort auf den Button mit den drei Punkten. Wähle die maximale Länge von 16 Zeichen und nutze den gesamten Zeichensatz.[224] Gehe die nächsten Eingabefelder durch und bestätige die Angaben jeweils mit *Weiter*. Lege aus Sicherheitsgründen eine Gültigkeitsdauer von maximal 6 Monaten für deine Kennwörter fest. Hast du alles Notwendige eingegeben, dann bestätige den Eintrag mit *Speichern*.

Benötigst du Benutzername und Kennwort beispielsweise für dein Web-Mail, dann tippe zuerst auf die Gruppe, dann auf den gesuchten Eintrag. Du findest den Eintrag auch über die Lupe im Kopfbereich von KeePass, indem du den Titel des Eintrages eingibst. Ist der Eintrag geöffnet, dann tippe noch oben rechts auf das Auge, damit das Kennwort sichtbar angezeigt wird. Aus Sicherheitsgründen solltest du die Keepass2Android-Tastatur verwenden oder die Passwörter für die jeweiligen Accounts manuell eintippen. Nutzt du Benutzername und Passwörter über die Zwischenablage, könnten Passwort-Sniffer diese abfangen. Unter den Anwendungs-Einstellungen kannst du festlegen, dass das Kopieren der Passwörter über die Zwischenablage deaktiviert bleibt. Sicherheit kostet Bequemlichkeit.

Tipps für Passwörter

- Je länger und komplexer das Passwort ist, um so sicherer ist es vor Angriffen. Wähle die maximale Länge von 16 Zeichen und nutze den gesamten Zeichensatz: Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen.
- Verwende für jedes Konto ein eigenes Passwort. Haben Angreifer ein Passwort gehackt, haben sie keinen Zugriff auf die übrigen Konten und können nicht etwa über dein Paypal-Konto auf Einkaufstour gehen.
- Ändere deine Passwörter regelmäßig, etwa jeden 6. Monat, sodass es Angreifer schwerer haben, deine Passwörter „irgendwann“ zu knacken.
- Sichere die Keepass-Datenbank auf einem externen Datenträger, wie USB-Stick, CF-Karte oder CD. Geht nämlich dein Handy verloren oder geht der interne Speicher kaputt, gehen auch gleich alle verschlüsselten Passwörter verloren.
- Hinterlege auf deinem KeePass2Android keine besonders vertraulichen Zugangsdaten, wie den OpenPGP-Schlüssel, die Passwörter für verschlüsselte Containerdaten, Kreditkartendaten oder PINs von EC-Karten. Gelingt es Angreifern mit einem Keylogger das Master-Passwort abzufangen, dann sind deine Passwörter schutzlos. Besser ist, du speicherst deine besonders vertraulichen Zugangsdaten in einem zweiten Passwort-Safe ab, den du nur auf deinem PC für Bankgeschäfte nutzt.

224 Die Qualität deiner Passwörter kannst du online überprüfen. Der Datenschutzbeauftragte des Kantons Zürich bietet hierzu einen Passwort-Check an: https://review.datenschutz.ch/passwortcheck/check.php. Die mit KeePass2Android erstellte Datenbank kannst du auch am PC mit dem kostenlosen Open-Source-Keyverwalter KeePass2.x nutzen.

Willst du die Datenbank schließen, dann tippe oben rechts das Schloss an und dann auf *Datenbank schließen*.[225]

Um erneut die Passwort-Datenbank zu entsperren, müsstest du jedes Mal dein langes und komplexes Passwort auf deiner Handytastatur eingeben – das ist unbequem, zeitraubend und fehleranfällig. Abhilfe schafft hier QuickUnlock. Öffne die Datenbank mit deinem sicheren Passwort und aktiviere *QuickUnlock*. Die App sperrt sich dann nach der in den *Einstellungen* vorgegebenen Zeit. Willst du die Datenbank wieder entsperren, dann gib die letzten 3 Zeichen (nach der Voreinstellung) deines Passwortes ein. Gibst du das falsche Kurzpasswort ein, ist die Passwort-Datenbank wieder verriegelt und sie muss wieder mit dem kompletten Passwort geöffnet werden. Ist QuickUnlock sicher? Solltest du dein Handy verlieren und sollte jemand versuchen per QuickUnlock die Passwort-Datenbank zu öffnen, hat er dazu nur eine Chance. Verwendest du als Kurzpasswort 3 Zeichen und als Zeichensatz die 30 Groß- und Kleinbuchstaben des deutschen Alphabets sowie 10 Ziffern, ergibt dies 70 mögliche Zeichen. Der Unberechtigte hat in diesem Fall eine Chance von 0,000003 Prozent die Datenbank zu öffnen. Ist dir die Chance für einen erfolgreichen Angriff noch zu groß, erhöhe das Kurzpasswort auf 4 Zeichen und die Chance sinkt auf 0,00000004 Prozent.

4.6.4 Daten sicher löschen

Schutz der digitalen Privatsphäre heißt, die eigenen Daten unter Kontrolle zu haben. Löschst du Daten auf deiner microSD-Karte, werden diese nicht wirklich gelöscht, sondern es wird nur Speicherplatz freigegeben. Die gespeicherten Informationen im Hintergrund bleiben so lange abrufbar, bis sie mit neuen Daten überschrieben werden. Mit Datenrettungstools wie Recuva[226] können gelöschte Dateien wieder zum Vorschein gebracht werden. Verschenkst oder verkaufst du dein Smartphone oder willst du es lediglich entsorgen, solltest du die darauf befindlichen Daten sicher löschen.

Android auf Werkeinstellung zurücksetzen

Erste Maßnahme: Setze dein Smartphone wieder auf Werkeinstellung zurück; das ist der Zustand des Neukaufs und bedeutet, dass sämtliche Daten, installierten Apps und Einstellungen gelöscht werden. Die Werkeinstellung findest unter: *Menü/Einstellungen/Sichern und Zurücksetzen*. Unter dem Punkt *Persönliche Informationen* findest du die Schaltfläche *Auf Werkeinstellungen zurücksetzen*. Berühre die Schaltfläche und be-

225 Heise Security meldet, dass aus einer Studie der Leibniz Universität Hannover hervorgeht, dass Passwortmanager auf Android „nicht sehr sicher“ sind, weil eine dazu erforderliche Schnittstelle (API) fehlt: http://www.heise.de/security/meldung/Fehlende-Schnittstelle-macht-Smartphone-Passwortmanager-unsicher-1830188.html

226 http://www.piriform.com/recuva/download

stätige nochmals mit *Gerät zurücksetzen*. Willst du wirklich sichergehen, kannst du dich auf *Werkeinstellungen zurücksetzen* nicht verlassen, da hierbei die alten Daten nicht mit Zufallsdaten überschrieben werden. Mit Forensik-Tools wie DEFT[227] lassen sich die Daten wiederherstellen.

Maßnahmen zum sicheren Datenlöschen

Zweite Maßnahme: Lösch-Tools hingegen geben nicht nur den Speicherplatz frei, den die zu löschende Datei belegt hat, sondern überschreiben den Speicherplatz mit zufälligen Daten. Durch das Überschreiben der Datei oder des gesamten Datenträgers wird eine Wiederherstellung der Daten unmöglich.

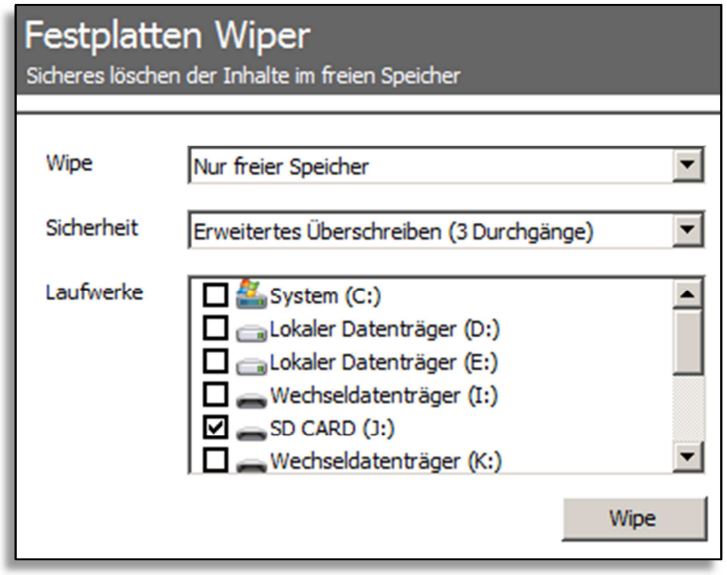


Abb. 30: Festplatten Wiper von CCleaner

So geht's: Sind die vertraulichen Daten auf der microSD-Karte abgespeichert, dann kannst die die Speicherkarte mithilfe eines Adapters und Kartenlesers über den PC fürs Erste neu formatieren. Hast du die Speicherkarte formatiert, kannst du den freien Speicher mit der Freeware CCleaner[228] auch über mehrere Löschvorgänge mit Datenmüll überschreiben. Starte das Lösch-Tool. Unter *Extras/Festplatten Wiper* kannst du die Einstellungen zum Löschvorgang vornehmen. Drei Durchgänge sollten fürs sichere Löschen ausreichen. Mit dem Klick auf *Wipe* startet das Tool mit dem Überschreiben des freien Speichers. Eine Alternative zu CCleaner ist das Open-Source-Tool Eraser.[229] Und so geht's: Bevor du den freien Speicherplatz shredderst, musst du unter *Settings* die Löschdurchgänge festlegen. Mach nun im Explorer-Fenster des PCs einen Rechtsklick auf das Laufwerk mit der microSD-Karte. Im Kontextmenü klickst du auf *Eraser/Erase Unused Space*. Wie lange der Löschvorgang dauert, hängt von der gewählten Löschmethode sowie der Schreibgeschwindigkeit der Karte ab.

Wie kann man die Handydaten auf dem Festspeicher sicher löschen? Der beste Weg ist, du verschlüsselst dein Handy mit den Android-Bordmitteln. Wähle hierzu im Menü den Punkt *Sicherheit/Telefon verschlüsseln/Telefon verschlüsseln.* Ist die Verschlüsselung abgeschlossen, setze dein Handy auf Werkeinstellung zurück. Mit dem Werks-Reset wird der Schlüssel vernichtet und die Handydaten können nicht entschlüsselt

227 Das Digital Evidence & Forensics Toolkit, kurz DEFT, ist ein Live-System auf Linux-Basis, das eine Sammlung von spezialisierten Tools für den IT-Forensiker enthält: http://www.deftlinux.net/
228 https://www.piriform.com/ccleaner
229 http://eraser.heidi.ie

werden. Richte dann dein Handy ohne Angabe von WLAN- oder Konto-Daten neu ein. Decke anschließend die Kameralinse mit einem Klebestreifen ab und lasse danach die Videokamera so lange laufen, bis der freie Speicher komplett mit Videodaten überschrieben ist. Setze abschließend das Handy wieder auf Werkzustand zurück. Das so bereinigte Handy kannst du bedenkenlos verschenken oder bei eBay versteigern, ohne befürchten zu müssen, dass der spätere Besitzer deine Handydaten wieder herstellen kann.

4.7 Schutz der Verfügbarkeit

Gefahren: Datenverlust kann jeden Nutzer treffen. Das Speichermedium des Handys kann kaputt gehen und SMS, E-Mails, Mailadressen, Telefonbuch und Fotos können verloren sein. Auch ein unbedachter Tipp auf den Lösch-Knopf auf dem Android genügt. Mit regelmäßigen Backups sicherst du deine persönlichen Daten für den Notfall und mit Datenrettern können verloren geglaubte Daten oftmals wieder hergestellt werden.

Backups erstellen: Es gibt mehrere Methoden, um Backups für Android zu erstellen. In der Regel liefert jeder Handyhersteller auch ein Backup-Tool mit, mit dem du die wichtigsten Daten auf dem PC sichern kannst. Die Datensicherung kann auch über das Google-Konto[230] erfolgen, sofern du über ein solches verfügst. Die Android-Einstellungen findest du unter *Sichern & zurücksetzen*. Legst du dir ein neues Handy zu, dann kannst du über das Backup-Konto Einstellungen, Apps und Kontakte direkt auf das neue Handy aufspielen. Google-Server sind als Cloud-Speicher nicht alternativlos. Für Privatanwender gibt es bei vielen Cloud-Anbietern kostenlosen Speicherplatz. Der Cloud-Dienst TeamDrive[231] bietet neben Speicherplatz auch eine Ende-zu-Ende-Verschlüsselung, so dass Verfügbarkeit und Vertraulichkeit der Daten gleichzeitig gewährleistet sind.

Deine Android-Daten kannst du auch über eine Desktop-Software auf dem PC sichern. Der Vorteil liegt darin, dass zureichender Speicherplatz zur Verfügung steht und dass persönliche Daten nicht auf fremden Servern liegen. Eine einfach zu bedienende Desktop-Software ist MyPhone Explorer.[232] In Verbindung mit dem Smartphone-Client MyPhoneExplorer Client[233] können Kontakte, SMS, Anruflisten und Fotos auf dem PC gespeichert werden.

Verwende für besonders schützenswerte Daten als Backup-Medium verschiedene Datenträger, wie USB-Stick, externe Festplatte oder DVD. Bewahre eines der Backup-Medien außer Haus auf, etwa in einem Bankschließ-

230 https://accounts.google.com/signup
231 http://www.teamdrive.com/de. Eine Kurzanleitung zu TeamDrive findest du im Abschnitt „Cloud verschlüsseln“.
232 http://www.fjsoft.at/de/home.php
233 MyPhoneExplorer Client wird in Google Play angeboten.

fach. Denn eine Sicherheitskopie auf einem Datenträger, der bei einem Brand- oder Wasserschaden in der eigenen Wohnung auch zerstört wird, nützt nichts.

Daten retten: Gelöschte Daten sind nicht wirklich gelöscht, sie können lediglich vom Betriebssystem nicht mehr ausgelesen werden. Der eigentliche Inhalt der Datei existiert so lange, bis der Inhalt mit anderen Daten überschrieben wird. Mit Tools wie Android Data Recovery[234] können in vielen Fällen gelöschte Daten wie SMS, Kontakte oder Fotos vom Android-Handy wiederhergestellt werden. Das Recovery-Tool rettet auch Daten, die durch Zurücksetzen auf Werkeinstellung oder Rooten verloren gegangen sind. Dabei muss das Handy über die USB-Debugging-Funktionen von Android mit dem PC verbunden werden. Speichere die geretteten Daten nicht auf dem Speichermedium, wo sich die zu rettenden Daten befinden. So vermeidest du, dass die gelöschten Dateien überschrieben werden und nicht mehr gerettet werden können.

4.8 Schutz der Anonymität

> *„Wenn es etwas gibt, von dem Sie nicht wollen, dass es irgendjemand erfährt, sollten Sie es vielleicht ohnehin nicht tun."*
>
> Eric Schmidt, Informatiker und Manager

Gefahren: Wer das Internet nutzt, hinterlässt Datenspuren. Rufst du eine Webseite auf, sieht der Webserver die IP-Adresse, über die dein Browser die Anfrage gesendet hat. Wer hinter der IP-Adresse steht, weiß der Access-Provider, mit dem du den Providervertrag abgeschlossen hast. Vermarkter nutzen Cookies und Tracking-Dienste, um zu ermitteln, wen, was, wie lange im Netz interessiert und welche Artikel Nutzer letztlich in den Warenkorb legen. Werden all die Datenspuren zusammengefügt, erhält der Nutzer ein unverwechselbares Gesicht, das für zielgerichtete Werbung verwendet werden kann. Den Ermittlungsbehörden dienen die Datenspuren dazu, Straftaten aufzuklären und Gefahren abzuwehren. Damit ist aber das Grundrecht des Nutzers auf Anonymität verletzt. Das Recht anonym zu handeln, kann aus dem Recht der Persönlichkeitsentfaltung (Art. 2 Verf.), Unverletzlichkeit der Wohnung (Art. 14 Verf.), Telekommunikationsgeheimnis (Art. 15 Verf.) sowie Meinungsfreiheit (Art. 21 Verf.) hergeleitet werden. Anonym im Netz handeln heißt, selbst bestimmen zu können, für wen man identifizierbar ist. Anonymität ermöglicht beispielsweise investigativen Journalismus. Ein Informant, der identifiziert werden kann, gibt seine nachweisbaren Informationen zu Korruption, Machtmissbrauch oder Gesetzesverletzungen (möglicherweise) nicht weiter.[235] Politische Repression kann Menschen davor abhalten, in Blogs oder Foren die Regierung offen zu kritisieren.

234 Webseite des Entwicklers: http://www.aiseesoft.de/android-data-recovery/
235 Die Enthüllungsplattform WikiLeaks (http://wikileaks.org/) wäre ohne Anonymität nicht möglich gewesen.

Abhilfe durch „Tarnkappen“: Technischen Schutz für (nahezu) anonyme Kommunikation im Netz bieten Anonymisierer, wie das Tor-Projekt.[236] Mit einem Anonymisierer wie Tor wird die IP-Adresse des Internetnutzers verschleiert, indem zwischen dem PC des Anfragers und dem Webserver eine Kette von Proxyservern geschaltet wird. Ruft der Nutzer eine Webseite auf, verbindet er sich verschlüsselt mit dem Entry Guard (Eintrittspunkt) des Tor-Netzwerkes. Dieser reicht die Anfrage verschlüsselt an einen Relay Node (Weiterleitungspunkt) weiter. Der zweite Knoten kennt nur die IP-Adresse des Entry Guard. Der Relay Node leitet die Anfrage schließlich an den Exid Node (Austrittspunkt) des Tor-Netzwerkes weiter. Der Exid Node kennt nur die Webadresse der Anfrage, aber nicht die eigentliche Quelle. Der Webserver, an den die Anfrage letztlich gerichtet ist, sieht nur die IP-Adresse des Exit Nodes. „Lauscher“ können so nicht rückverfolgen, wer der Anfrager ist. Voraussetzung ist aber, dass die Anonymisierungssoftware selbst vertrauenswürdig ist.

Are you using Tor? | https://ch…
Congratulations. Your browser is configured to use Tor.
Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously.
Abb. 31: Orbot anonym surfen

Das Anonymisierungsprogramm Tor gibt es für Windows, Mac oder Linux. Lade dir am besten das gesamte Tor-Browser-Firefox-Paket vom Tor-Projekt herunter.[237] Das Tor-Paket ist auch von einem USB-Stick aus lauffähig. Du kannst Firefox mit zusätzlichen Add-ons, wie Adblock Plus, Cookie Monster, Noscript oder Disconnect erweitern, um ungebetene Werbung und Tracking-Dienste zu blockieren.[238] Erstelle noch von deinem Installationsverzeichnis eine Desktop-Verbindung, dass du mit einem Doppelklick auf *Start Tor Browser* das Programm nutzen kannst. Loggst du dich mit Tor bei deiner Bank, auf Facebook oder deiner Webmail ein, ist es um die Anonymität geschehen. Mit den Login Daten gibst du preis, wer die Anfragen durch das Tor-Netzwerk schickt.[239]

Mit der App Orbot, der Mobilversion des Tor-Browsers, sowie der Browser-App Orweb kannst du auch mit Android-Handys anonym surfen.[240] Orbot leitet alle Internetzugriffe über das *Tor*-Netzwerk um. Hast du Orbit installiert, musst du die App erst noch richtig konfigurieren. Nach dem Start hilft dir ein Assistent beim Einrichten. Du kannst den gesamten Datenverkehr über das Tor-Netzwerk leiten oder nur bestimmte Apps. Im Menü unter dem Punkt *Einstellungen/Transparent Proxying/Select Apps* findest du eine Liste aller

236 https://www.torproject.org/
237 https://www.torproject.org/projects/torbrowser.html.en
238 Johannes Endres (2013): *Tracking-Schutz im Browser,* in: c’t Security 2013, S. 124-125.
239 Internetnutzer, die noch mehr Sicherheit beim Surfen wünschen, booten von einer Live-CD oder einem Live-USB-Stick. Tails (https://tails.boum.org/) ist beispielsweise ein Linux-System, das speziell fürs anonyme Surfen im Netz ausgerichtet ist. Tor ist mit an Bord. Der Vorteil einer Live-CD ist, dass der Anwender bei jedem Start mit der Werkseinstellung startet. Cookies oder Schadcode haben so keine Chance sich ins System einzunisten. Wer ganz auf der sicheren Seite sein will, sollte nicht das heimische Netzwerk nutzen, sondern am besten ein öffentliches WLAN.
240 Orbot und Orweb findest du auf Google Play.

installierten Apps auf deinem Handy. Setze einfach ein Häkchen hinter den Apps, die über das Anonymitäts-Netzwerk geleitet werden sollen.

Die Verbindung zum Tor-Netzwerk stellst du mit einem langen Fingertipp auf das Orbot-Symbol in der Mitte des Displays her. Überprüfe, ob die Verbindung tatsächlich steht. Tippe dazu auf die Weltkugel in der oberen, rechten Ecke des Displays. Funktioniert alles, öffnet sich ein Browser-Fenster, das die Tor-Verbindung anzeigt.[241] Völlig anonym mit dem Handy bist du jedoch auch mit Anonymisierern nicht. Als Handynutzer bist du über die Standortdaten, Rufnummer oder SIM-Kartennummer identifizierbar.

241 Das Tor-Netzwerk bietet offenbar keine 100-prozentige Sicherheit, vgl. Jürgen Schmidt (2013): *Eigen-Tor. Gefahren der Tor-Nutzung im Alltag,* in: c’t 2013 Heft 20, S. 102. Holger Bleich (2013): *Mythos Anonymität. Von der Schwierigkeit, sich unerkannt im Internet zu bewegen,* in: c’t 2013 Heft 20, S. 96-101.

4.9 Handy-Tipps, Plattformen, Apps

Tipps für die Handy-Praxis

Telefonierst du oder nutzt du das Internet mit einem Smartphone, solltest du in deinem eigenen Interesse ein paar Regeln beherzigen und Maßnahmen zum Selbstschutz treffen, damit du dein digitales Leben effektiv selbst bestimmen kannst.

Deine Daten gehören dir!
Überlege dir, was du über dich wem mitteilst. Wähle für deine E-Mail-Adressen sowie für Benutzernamen in Chats und sozialen Netzwerken ein Pseudonym, das keine Rückschlüsse auf deinen tatsächlichen Namen zulässt. Die Vermarkter sammeln Daten, um wirksamere Werbung zu schalten; dubiose Händler verkaufen Nutzerdaten. Kriminelle sind an deinen Konto- und Kreditkartendaten interessiert. Behalte die Kontrolle über deine persönlichen Daten.

PIN oder Passwort einrichten
Richte eine PIN oder ein Passwort für die Bildschirmsperre ein, um dein Handy vor unbefugten Zugriffen zu schützen. Aktiviere auch *Automatisch sperren*, sodass der Zugriffschutz auch im Ruhezustand aktiviert wird.

Daten und Kommunikation verschlüsseln
Sollen deine Telefonate nicht belauscht und Chats nicht mitgeschnitten werden oder deine vertraulichen Daten vertraulich bleiben, dann solltest du Kommunikation und Daten verschlüsseln. Als digitale Schutzschilder kannst du EDS für deine Daten, Threema für deine Chats und RedPhone für deine Telefonate verwenden. Willst du dein Handy verkaufen oder entsorgen, solltest du zuvor alle vertraulichen Daten sicher löschen.

Aktiviere Netzverbindungen nur bei Bedarf
Schalte die Dienste wie WLAN und Bluetooth ab, wenn du sie nicht benötigst. Damit stellst du sicher, dass sich dein Handy nicht unbemerkt in einen manipulierten Hotspot einloggt. Je weniger Angriffsfläche du dem Angreifer bietest, desto geringer ist das Risiko, dass der Angriff erfolgreich ist.

Installiere nur Apps aus vertrauenswürdigen Quellen
Lade dir Apps nur aus dem offiziellen App-Store (Google Play) herunter. Installierst du Apps von Drittanbietern, solltest du zuvor in jedem Fall einen App-Check durchführen. Gibt es ein Impressum vom Entwickler, gibt es ausreichende Nutzerkommentare, wurde die App von Security-Plattformen getestet? Angreifer versuchen nämlich über infizierte Apps, Schadcode auf das Smartphone einzuschleusen.

Überprüfe die Zugriffsrechte der Apps
Kontrolliere, welche Zugriffsrechte die App anfordert. Überlege, ob die Berechtigungen (Zugriff aufs Telefonbuch, SMS-Versand, Standortdaten) wirklich für die Funktionsweise der App notwendig sind. Apps können sich als Horchposten für deine Daten entpuppen.

Kontrolliere die Identität des Webseiten-Anbieters
Vergewissere dich bei Internetsitzungen, dass du dich tatsächlich auf der Webseite des Anbieters befindest. Das ist besonders wichtig bei Bankgeschäften, Abschluss von Verträgen oder beim Herunterladen von Software und Apps. Die Identität des Anbieters kannst du über das Zertifikat des Anbieters prüfen – mit Klick auf das Schlosssymbol im Browser.

Handyquette

1. Telefonate stören anwesende Personen. Ein laufendes Gespräch wird unterbrochen und die Anwesenden müssen unfreiwillig ein Privatgespräch mithören. Deshalb sind Telefonate während des Essens oder bei Besprechungen tabu.
2. Telefoniere nicht an Orten der Ruhe und Konzentration, wie etwa in Bibliotheken, bei Vorträgen oder auf Kunstausstellungen.
3. Telefoniere nicht beim Fahrrad- oder Mopedfahren; du kannst dich nicht gleichzeitig auf das Telefonat und den Straßenverkehr konzentrieren und kannst deshalb dich und andere Verkehrsteilnehmer gefährden.
4. Eine Unsitte ist, das Handy während eines Tischgesprächs lautlos zu schalten und alle 30 Sekunden darauf zu schauen, ob eine Nachricht eingegangen ist. Damit zeigst du, dass dir etwaige Mitteilungen wichtiger sind als dein Gegenüber.
5. Im eigenen Interesse solltest du Handy-Auszeiten festlegen. Ohne Pops über eingehende E-Mails, SMS oder Status-Updates lassen sich Hausaufgaben und wichtige Projekte konzentrierter bearbeiten.

Führe Sicherheitsupdates durch
Führe regelmäßig für das Betriebssystem und die installierten Apps Updates durch, sodass Schadcode nicht über bekannte Sicherheitslücken auf dein Smartphone gelangen kann.

Installiere ein Antiviren-Programm
Installiere ein aktuelles Antiviren-Programm. Es gibt von den großen Softwarehäusern auch kostenlose Programme. Sieh dir zuvor aktuelle Tests an; die Leistungsfähigkeit der Programme kann sich innerhalb von Monaten ändern.

Sei vorsichtig beim Bezahlen mit dem Handy!
Die Bezahlung per Handy ist bei Kleinbeträgen, etwa bei Spenden für Hilfsaktionen, eine bequeme Zahlungsart. Der Bezahlung erfolgt per Anruf einer kostenpflichtigen Nummer oder über eine Premium-SMS. Überprüfe dein Handy daraufhin, ob sich im Hintergrund böswillige Apps eingenistet haben, die selbstständig kostenpflichtige Rufnummern anwählen oder SMS versenden. Kontrolliere deine Mobilfunkabrechnung nach falschen Abbuchungen. Ist dies der Fall, melde den Betrug deinem Mobilfunknetzbetreiber und der Post- und Kommunikationspolizei.

Notiere dir die Gerätenummer (IMEI)
Notiere dir die Seriennummer des Handys, damit du es nach dem Verlust wieder identifizieren kannst. Die Gerätenummer kannst du mit der Eingabe *#06# abfragen.

Halte dich auf dem Laufenden!
Die Online-Welt ist ständig in Bewegung. Was gestern noch aktuell war, kann heute überholt sein. Informiere dich stets darüber, was es Neues gibt zu Chancen und Risiken der Internetnutzung, zu Fragen der Privacy, Betrügereien oder Schadcode. Kennst du die potentiellen Risiken des Netzes, machst du dich nicht selbst leichtfertig zum „gläsernen Nutzer“ und kannst geeignete Abwehrmaßnahmen treffen. Es gibt eine Reihe von Internetradios, die über die digitale Welt laufend per Podcast informieren:

N-JOY: http://www.n-joy.de/radio/njoypodcasts103.html;
Chaosradio: http://chaosradio.ccc.de;
Digital: http://www.srf.ch/wissen/digital/specials/computer-im-beruf
Ö1 Digital.Leben: http://oe1.orf.at/podcast/?page=2

Plattformen zur Medienkompetenz

Titel	Webadresse	Inhalt
Chaosradio	http://chaosradio.ccc.de	Chaosradio ist eine monatliche Radiosendung des Chaos Computer Club (CCC). Die Radiosendungen behandeln Themen rund um digitale Technologien, Schutz der Privacy und Gesellschaft. Die einzelnen Sendungen stehen als Livestream und als Podcast im Netz zur Verfügung.
Handywissen.at	http://handywissen.at	handywissen.at geht aus einer EU-Initiative für sichere Handy- und Internetnutzung hervor. Die Plattform stellt hierfür Infos für Eltern und Lehrende hierfür bereit.
JFF - Institut für Medienpädagogik	http://institut-medienpaedagogik.de	Unter der Rubrik „Webhelm“ stehen Materialien zu Themen des Web 2.0 zur Förderung der Medienkompetenz Jugendlicher sowie methodische Anregungen für pädagogische Fachkräfte zur Verfügung.
„iRights.info“	www.irights.info	iRights.info ist eine Plattform, die sich mit kritischen Analysen zum Urheberrecht und kreativen Werken in der digitalen Welt beschäftigt.
Klicksafe.de	https://www.klicksafe.de	Klicksafe ist eine EU-Initiative für mehr Sicherheit im Netz. Ziel ist, Internetnutzer zu befähigen, die Neuen Medien handlungskompetent und kritisch zu nutzen.
Lehren und Lernen im 21. Jahrhundert	http://agora-wissen.blogspot.de/	Blog, der regelmäßig aus dem Themenbereich „PC, Internet und Web 2.0 in Forschung und Lehre, Schule und Hochschule“ berichtet.
N-JOY	http://www.n-joy.de/radio/njoypodcasts103.html	N-JOY ist ein Radioprogramm, das sich täglich mit Themen der digitalen Welt beschäftigt, wie Datenschutz, Privacy, Apps für Smartphones oder Geschäftspraktiken. Die einzelnen Radiosendungen werden auch als Podcast angeboten.
Safer Internet	http://www.saferinternet.at	Safer Internet ist Teil des Safer-Internet-Programms der Europäischen Union. Ziel des Projekts ist, bei Jugendlichen, Eltern und Lehrern die Medienkompetenz zu fördern.

Tab. 14: Plattformen zu Medienkompetenz

App-Tipps

Bezeichnung	App-Anbieter/-Entwickler	Kurzbeschreibung
Aldiko Book Reader	https://play.google.com/store http://www.aldiko.com/	Aldiko Book Reader ist eine E-Book-App, welche die Formate EPUB und PDF mit oder ohne Adobe DRM-Schutz unterstützt. Die App kann u. a. die Schriftgröße, -art und -farbe verändern und sich die Leseposition merken.
avast Mobile Security	https://play.google.com/store http://www.avast.com/de-de/index	avast Mobile Security ist ein Virenscanner für Handys, der Apps und Daten nach Schadcode überprüft. Zudem ist ein sogenannter Antidiebstahlschutz eingebaut, mit dem der Besitzer das Handy orten kann.
BitTorrent Sync	https://play.google.com/store https://www.getsync.com/	BitTorrent Sync ist ein Tool für die private Cloud. Sie garantiert durch die Ende-zu-Ende-Verschlüsselung ein hohes Maß an Sicherheit.
BoxCryptor	https://play.google.com/store https://www.boxcryptor.com	BoxCryptor verschlüsselt vertrauliche Daten, bevor sie auf den Cloud-Server hochgeladen werden. Ist BoxCryptor installiert, werden alle Daten im BoxCryptor Laufwerk verschlüsselt und im lokalen Ordner des Cloud-Dienstes abgespeichert. Mit dem Cloud-Dienst werden dann nur mehr die verschlüsselten Dateien synchronisiert.
ChatSecure	https://play.google.com/store https://guardianproject.info/apps/chatsecure	ChatSecure ist eine Open-Source-App, die Chats verschlüsselt. Die App ist so wie Orbot Teil des The Guardian Project, das sich dem Schutz der digitalen Privatsphäre verschrieben hat.
ECC-Net Travel	https://play.google.com/store http://www.eu-verbraucher.de/en/publications/app	ECC-Net Travel ist ein Projekt des Netzwerks der Europäischen Verbraucherzentren und unterstützt Reisende darin, ihre Verbraucherrechte im Ausland geltend zu machen.
EDS	https://play.google.com/store http://www.sovworks.com	EDS (Encrypted Data Store) ist eine Security-App, mit der Nutzer verschlüsselte Datencontainer erstellen können.
Firefox	https://play.google.com/store http://www.mozilla.org/de/firefox/fx	Firefox ist ein alternativer Browser fürs Handy. Der Vorteil von Firefox liegt darin, dass man ihn mit Erweiterungen wie Adblock Plus an eigene Interessen anpassen kann, etwa um Werbung zu blockieren.

Bezeichnung	App-Anbieter/-Entwickler	Kurzbeschreibung
IMDb Filme & TV	https://play.google.com/store http://www.imdb.com/	IMDb ist Informationsquelle zu Filmen und TV-Serien. Die App liefert eine Kurzinfo zu Handlung, den beteiligten Schauspielern und zeigt Bewertungen an.
K-9 Mail	https://play.google.com/store https://code.google.com/p/k9mail http://www.openkeychain.org	K-9 Mail ist ein Open-Source-E-Mail-Client sowohl für POP3- als auch für IMAP-Konten. In Verbindung mit Open-Keychein können E-Mails verschlüsselt und signiert werden.
KeePass2Droid	https://play.google.com/store http://keepass2android.codeplex.com	KeePass2Droid ist ein quelloffener Passwortmanager, mit dem sichere Passwörter erzeugt und verwaltet werden können. Die App nutzt das Datenbank-Format, das auch von der Desktop-Software KeePass 2.xx für Windows und andere Betriebssysteme verwendet wird.
Label-online	https://play.google.com/store http://label-online.de/	Label-online ist eine App zum schnellen Label-Check für den ethischen Einkauf. Labels auf Produkten werden fotografiert und die App informiert, wofür das Label steht und ob es glaubwürdig ist.
LibreOffice Viewer	https://play.google.com/store https://www.documentfoundation.org/	LibreOffice Viewer ist eine App, mit der sich Dokumente ansehen und bearbeiten lassen. Die App unterstützt das offene ODF-Format sowie die Dateiformate von MS-Office.
Menthal	https://play.google.com/store https://menthal.org/	Menthal-App misst die Smartphone-Nutzung. Die App sammelt Daten, wie oft der Nutzer das Handy entriegelt, wieviel Zeit er damit verbringt oder welche Apps er am häufigsten nutzt.
Orbot	https://play.google.com/store https://www.torproject.org/docs/android.html.en	Orbot leitet alle Internetzugriffe über das Tor-Netzwerk um. Mit der Umleitung wird die eigene IP-Adresse verschleiert. Die App ermöglicht anonymes Surfen.
RedPhone	https://play.google.com/store	RedPhone ist eine Open-Source-App, die Telefonate verschlüsselt. Die Gespräche werden nicht über das Mobilfunknetz, sondern über eine 3G- oder WLAN-Verbindung geleitet.
SRT AppGuard	http://www.srt-appguard.com/de	SRT AppGuad ist ein Wächter für Apps, der die Kontrolle über die Berechtigungen der installierten Apps ermöglicht und so für mehr Schutz der digitalen Privatsphäre sorgt.

Bezeichnung	App-Anbieter/-Entwickler	Kurzbeschreibung
StartPage Search	https://play.google.com/store https://www.startpage.com/	StartPage Search verschlüsselt Suchanfragen und verspricht die IP-Adresse des Anwenders nicht zu speichern. Die Suchergebnisse können per Proxy-Server anonymisiert aufgerufen werden.
TeamViewer	https://play.google.com/store http://www.teamviewer.com/de/index.aspx	TeamViewer ist eine App zur Fernsteuerung von PCs, Handys und Tablets. Nutzer können von unterwegs auf Daten und Programme ihres PCs zugreifen oder Freunden bei PC-Problemen helfen.
Threema	https://play.google.com/store https://threema.ch/de	Threema ist eine Kurznachrichten-App, die alle Nachrichten, auch Gruppen-Chats, Ende-zu-Ende verschlüsselt.
Total Commander	https://play.google.com/store http://www.ghisler.com/android.htm	Total Commander ist ein Dateimanager, mit dem man Dateien kopieren, verschieben, umbenennen, komprimieren und löschen kann. Die App ist zudem per Plug-ins erweiterbar, etwa eine WLAN- oder FTP-Erweiterung.
Wickr	https://www.mywickr.com/en/index.php	Wickr ist ein Instant-Messenger, mit dem man selbstzerstörende und verschlüsselte Nachrichten versenden kann.
WiFi Finder	https://play.google.com/store http://www.jiwire.com/android	WiFi-Finder ist eine nützliche App für unterwegs, um ins Internet zu gelangen. Der WiFi-Finder zeigt nämlich die in der Nähe gelegenen offenen WLANs auf einer Karte an. Vorsicht ist geboten bei öffentlichen WLANs; sie können für Hotspot-Angriffe genutzt werden.
Wikipedia Mobile	https://play.google.com/store	Wikipedia Mobil ermöglicht, unterwegs kostenlos und werbefrei auf die gesamten Artikel der Enzyklopädie Wikipedia zuzugreifen.
WordPress	https://play.google.com/store https://android.wordpress.org	WordPress ist eine App für Blogger. Nutzer können mit der App neue Einträge erstellen, Kommentare hinzufügen oder Bilder und Videos einstellen.

Tab. 15: App-Tipps

4.10 Arbeitsaufträge

1. Erkundigt euch, wie Ermittler bei Telefon- und Internetüberwachung konkret vorgehen.
   a) Welche Fragen arbeitet eine Ermittlungsgruppe ab, die sich etwa mit der Rauschgiftkriminalität befasst, bevor sie einen Antrag beim Staatsanwalt auf Telefonüberwachung stellt?
   b) Welche Checkliste geht der Staatsanwalt im Falle der Rauschgiftkriminalität durch, bevor er einen Antrag an die Gerichtsbehörde auf Telefonüberwachung stellt? Werden Fragen der Verhältnismäßigkeit gestellt? Werden Überwachungsgründe hinterfragt?
   c) Gibt es konkrete Anträge der Staatsanwaltschaft auf Telefon- oder Internetüberwachung, die von der Gerichtsbehörde zurückgewiesen wurden? Wenn ja, aus welchen Gründen?
   d) Findet eine systematische Erhebung der Erfolge der Telefonüberwachung bei den Ermittlungsbehörden statt?

2. Benötigt die Gerichtspolizei die PIN des Handyinhabers, um bei einem beschlagnahmten Handy Zugriff auf Telefonbuch und SMS zu erhalten?

3. Moderne Handys können auch die Standortdaten der Nutzer erfassen. Wer auf seinem Android-Handy den Standortdienst von Google aktiviert, willigt ein, dass „anonyme Standortdaten an Google gesendet“ werden.
   a) Was macht die Firma Google mit den Standortdaten der Handynutzer?
   c) Der Wissenschaftler Jerome E. Dobson gibt zu bedenken: „Wenn du weißt, wo jemand ist, weißt du auch bald, wer er ist.“ Überlegt, wie man aus Bewegungsdaten ein Persönlichkeitsprofil erstellen kann.
   d) Welche Handy-Daten lassen sich neben den Bewegungsdaten für die Ermittlung deines Persönlichkeitsprofils nutzen?

4. Apps sind vielfach datenschutzrechtlich problematisch. Überprüft, welche Freigaben die Facebook-App[242] auf dem Android-Smartphone einfordert.
   a) Welche Berechtigungen haben einen Bezug zu den Funktionen der App?
   b) Welche Berechtigungen haben offensichtlich keinen Bezug zu den Funktionen der App?
   c) Informiert Facebook den Nutzer darüber, für welche Zwecke die gesammelten Daten verwendet werden?

242 https://play.google.com/store/apps/details?id=com.facebook.katana

5. Eine Standardformel bei Forderung nach mehr staatlicher Überwachung lautet: „Wer nichts zu verbergen hat, hat auch nichts zu befürchten.“ Interpretiert und analysiert die Formel und stellt euch hierbei auch folgende Fragen:

   a) Auf welche Art von Geheimnissen bezieht sich die Aussage „Wer nichts zu verbergen hat …“? Geht es hierbei um die heimliche Geliebte? Um ein technisches Verfahren in einem Unternehmen? Um die Wahlstrategie einer Partei?
   b) Gilt die Aussage „Wer nichts zu verbergen hat …“ auch für Polizeibehörden oder Geheimdienste? Sind Staatsgeheimnisse grundsätzlich illegitim?
   c) Was besagt der Teilsatz „… hat auch nichts zu befürchten“? Wie muss eine Telefon- und Internetüberwachung geregelt sein, damit unbescholtene Bürger tatsächlich „nichts zu befürchten“ haben?
   d) Wer legt fest, welches Verhalten der Bürger als verdächtig und welches als unverdächtig gilt?
   e) Zeigt an historischen und aktuellen Beispielen auf, wie sich eine totalitäre Überwachung der Bürger auf ihre Lebensführung auswirkt.
   f) Was unterscheidet bei staatlicher Überwachung den liberalen Freiheitsstaat vom totalitären Polizeistaat?[243]

6. Smartphones ermöglichen es Bürgerjournalisten, Polizeieinsätze zu filmen und ins Netz zu stellen. Führt die „Überwachung von unten“ zu mehr Rechtsstaatlichkeit bei den Polizeieinsätzen? Was spricht gegen oder für die Überwachung der staatlichen Überwacher?

7. Radarwarn-Apps weisen Autofahrer auf mobile Geschwindigkeitsmessgeräte hin. Diskutiert aus der Sicht der Verkehrssicherheit, ob Radarwarn-Apps erlaubt oder nicht erlaubt sein sollen.

8. Passwort-Safes sind bequem, um Passwörter zu generieren und zu verwalten. Welchen Anforderungen sollte ein Passwort-Safe genügen, dass er als zuverlässig eingestuft werden kann?

9. Die anonyme Internetnutzung ist umstritten. Nehmt Stellung zu den Thesen der Kritiker und Befürworter. Diskutiert, wie das Grundrecht auf Anonymität im Netz und die Schutzpflicht des Staates, Internetnutzer vor Cyberkriminalität zu schützen, gegeneinander ausbalanciert werden sollen.

   a) Kritiker der Anonymität im Netz verweisen darauf, dass manche Internetnutzer im Schutz der Anonymität die Meinungsfreiheit als Freibrief für Mobbing, Gewaltaufruf, Hetze oder Steuerhinterziehung missbrauchen. Ermöglicht der Staat die anonyme Nutzung von Internetdiensten, schützt er indirekt Straftäter.

243 DVD-Tipps zur Überwachung: *„Das Leben der Anderen“* 2006, Florian Henckel von Donnersmarck, DVD, 137 Minuten; *„Minority Report“* 2010, Steven Spielberg, DVD, 141 Minuten; *„Die Truman Show“* 2003, Peter Weir, DVD, 99 Minuten.

b) Befürworter der Anonymität argumentieren, dass die anonyme Internetnutzung Teil des Grundrechtes auf informationelle Selbstbestimmung ist. Danach kann jeder selbst entscheiden, wer welche Daten wozu verwenden darf. So wie Anonymität im realen Leben gängig ist, etwa bei Barzahlungen im Einzelhandel, sollte sie auch im Netz möglich sein.

10. Welche gesellschaftlichen Gruppen haben ein Interesse auf anonyme Nutzung des Internets?

11. Wie würdest du dich im Internet verhalten, wenn alle Aktivitäten aufgezeichnet würden? Also, welche Webseiten du aufgerufen, welche Software du heruntergeladen, welche Videos du dir angesehen, was du in sozialen Netzwerken gepostet und mit wem du gechattet hast.

12. Die Rolle der Whistleblower ist umstritten. Für die einen sind sie „Verräter“, für die anderen decken sie Missstände in Unternehmen und in der öffentlichen Verwaltung auf. Loyalitätspflicht des Arbeitnehmers gegenüber dem Arbeitgeber und das Grundrecht auf Meinungsfreiheit stehen hier in einem Konflikt zueinander.

    a) Diskutiert, in welchen Fällen Arbeitnehmer das Recht haben sollten, die Presse über Missstände im Betrieb oder in der öffentlichen Verwaltung zu informieren.
    b) Zeigt auf, wie die Anonymität eines Whistleblowers gewährleistet werden kann; etwa wie dieser eine Word-Datei mit brisantem Inhalt der Presse übers Internet zuspielen könnte, ohne dass Rückschlüsse auf seine Identität möglich sind.

13. Die Anhänger der sogenannten „Quantified-Self“-Bewegung sammeln Daten über den eigenen Körper und das eigene Leben.

    a) Warum sammeln Personen freiwillig Daten über sich selbst?
    b) Welche Daten erheben „Selbstvermesser“?
    c) Was machen die „Selbstvermesser“ mit den erhobenen Daten?
    d) Wie können die „Selbstvermesser“ ihre digitale Privatsphäre schützen?
    e) Warum glauben Kritiker der „Quantified-Self“-Bewegung, dass diese Bewegung mehr Leistungsdruck bewirke, mehr Überwachung ermögliche und zu einer „Gesundheitsdiktatur“ führe?

14. Nehmt Stellung zum Konzept einer Kopfgeld-App. Die Regierung muss die Ausgaben kürzen und u. a. müssen auch die Ermittlungsbehörden sparen. Im Zuge der Web 2.0-Diskussion entwickelt eine Firma eine „Kopfgeld-App“. Der Bürger soll bei der Aufklärung von Straftaten mithelfen. Wer eine Regelwidrigkeit oder Straftat über die Kopfgeld-App aufklärt, erhält je nach Strafmaß vom Staat ein Entgelt. Der Bürger sichert per Handyfoto Beweise etwa vom Falschparken, trägt seine Personendaten sowie die Tatortumstände in die App ein und lädt alles auf den Bürger-Server hoch. Diskutiert nachfolgende Fragen:

a) Welche Auswirkungen hätte (vermutlich) eine Kopfgeld-App auf die Aufklärungsrate von Straftaten?
b) Wie würde sich (vermutlich) eine Kopfgeld-App auf die Lebensführung der Bürger auswirken?
c) Wie könnte eine Kopfgeld-App von den Bürgern missbraucht werden?
d) Sind ökonomische Anreize die richtigen Instrumente, um die Sicherheit der Bürger zu verbessern?

15. Recherchiert, wie die illegale Datenwirtschaft im Netz funktioniert.

a) Wie kommen Hacker an E-Mail-Adressen, Anrufnummern, Postanschriften, Kreditkartendaten, Benutzernamen und Passwörter?
b) Wie funktioniert der Identitätsdiebstahl?
c) Wie funktioniert die Phishing-Methode?
d) Wie machen Cyberkriminelle persönliche Daten zu Geld?
g) Erstellt ein Schaubild zur illegalen Datenwirtschaft im Netz.

16. Vermarkter gehen von der Annahme aus, dass präzise Kundenprofile und gezielte Werbung Umsatz und Profit steigern. Analysiert wie Kundenprofile entstehen. Diskutiert die Frage, „Wer bin ich?“ Nehmt Stellung zu den nachfolgenden Thesen. Ergänzt die Thesen, falls sie für euch nicht schlüssig sind.

a) „Ich bin, was ich mir ansehe.“ (City Bike, iPhone)
b) „Ich bin, was ich gekauft habe.“ (Gebrauchtauto, Zugfahrkarte, Biolebensmittel)
b) „Ich bin, was ich mir vorstellen kann.“ (Beruf, Schulabschluss, Beziehung)
c) „Ich bin, was ich mache.“ (Alleinerzieher, Hacker, Snookerspieler)
e) „Ich bin, an was ich glaube.“ (Religion, Weltverbesserung)
f) …

17. Dein Smartphone weiß, wo du dich befindest und gibt die Standortdaten weiter. In Empfang nehmen diese der Mobilfunkbetreiber, der Hersteller des Betriebssystems sowie die Anbieter von Apps. Ermittle:

a) über welche Wege die Standortdaten eingesammelt werden können;
b) wie du die Ortung des Smartphones ausschalten kannst – für Mobilfunkbetreiber, Hersteller des Betriebssystems sowie App-Anbieter;
c) welche Apps die Standortdaten erst dann abfragen, nachdem du der Weitergabe ausdrücklich zugestimmt hast.

18. Apps zum Schutz der digitalen Privatsphäre sollen höchsten Anforderungen genügen. Erstellt einen Fragenkatalog, den Nutzer abarbeiten sollten, bevor sie sich für eine Security-App entscheiden.

a) Verfasst Fragen zu rechtlichen Aspekten.
b) Verfasst Fragen zur Sicherheit der App.

19. Dein Smartphone weiß, wo du dich befindest und gibt die Standortdaten weiter. In Empfang nehmen diese der Mobilfunkbetreiber, der Hersteller des Betriebssystems sowie die Anbieter von Apps. Ermittle:

    a) über welche Wege die Standortdaten eingesammelt werden können;
    b) wie du die Ortung des Smartphones ausschalten kannst – für Mobilfunkbetreiber, Hersteller des Betriebssystems sowie App-Anbieter;
    c) welche Apps die Standortdaten erst dann abfragen, nachdem du der Weitergabe ausdrücklich zugestimmt hast.

20. Das Handy ist zu einem mobilen Kommunikationsgerät geworden. Verfasst in drei Gruppen eine Handyquette für unterschiedliche Lebenssituationen. Diskutiert in der Klasse Handy-Regeln und hängt sie ans Schwarze Brett eurer Schule.

    Gruppe A verfasst eine Handyquette im Job.

    a) Wann sollte das Handy in jedem Fall ausgeschaltet bzw. auf lautlos gestellt sein?
    b) Wie lange darf ein Handy klingeln?
    c) Was tun, wenn man bei einem Arbeitsgespräch dringend auf einen Anruf wartet und es klingelt?
    d) Wie lange darf man telefonieren, wenn man während eines Arbeitsgespräches einen Anruf von einer Freundin erhält?
    e) …

    Gruppe B verfasst eine Handyquette für Freunde.

    a) Wann sollte das Handy beim Zusammensein mit Freunden ausgeschaltet sein?
    b) Bei welchen Veranstaltungen sollte das Handy auf lautlos gestellt sein?
    c) Wie lange darf man mit einer Freundin telefonieren, während man mit einer anderen Freundin im Kaffee sitzt?
    d) …

    Gruppe C erstellt Regeln für den Handy-Nutzer selbst und überlegt, warum eine Handy-Auszeit für den Handy-Nutzer sinnvoll sein könnte.

    a) Wann wäre eine Handy-Auszeit sinnvoll (nachts, zu Essenszeiten, Hausaufgaben, Urlaub …)?
    b) Wann sollten Pushmails oder sonstige Handy Push-Nachrichten wie Facebook-Statusmeldungen abgeschaltet werden?
    c) …

21. Der Schutz der Privatsphäre im Internet ist nicht unumstritten. Die Anhänger der „Privacy“ fordern eine Modernisierung des Datenschutzes, die des „Post-Privacy“ sehen im Schutz der Privatsphäre ein Auslaufmodell. Erstellt zu den beiden Grundpositionen Thesen und diskutiert sie.

Gruppe A beschäftigt sich mit dem Privacy-Konzept und geht insbesondere auf die Fragen ein, warum die Privatsphäre ein schutzwürdiges Gut ist und ob sich ihr Schutz im Umfeld von Google-Diensten, wie Google-Suchmaschine, Google Street View oder Facebook & Co noch wirksam durchsetzen lässt.

Gruppe B befasst sich mit dem Post-Privacy-Konzept und zeigt auf, welche Freiheiten und Möglichkeiten sich für Staat, Wirtschaft und einzelnen Bürger mit der umfassenden Transparenz aller Daten ergeben. Die Gruppe stellt sich auch die Frage, ob es Anzeichen für einen „historischen Trend“ hin zu einer transparenten Gesellschaft gibt.

22. Die Vorratsdatenspeicherung ist politisch umstritten. Überprüft, ob die nachfolgenden Thesen zur Vorratsdatenspeicherung belegt sind und diskutiert, ob sie mit den Grundrechten der Bürger vereinbar sind.

    a) Die Vorratsdatenspeicherung ist zur Aufklärung von Straftaten unabdingbar. Gibt es hierzu Daten bei den örtlichen Ermittlungsbehörden?
    b) Die Vorratsdatenspeicherung wird nur zur Bekämpfung schwerster Straftaten eingesetzt. Trifft dies tatsächlich zu? Welche Erkenntnisse hierzu haben Strafverteidiger oder Ermittlungsbehörden?
    c) Den Strafermittlern muss jedes technische Instrument zur Aufklärung und Verfolgung von Straftaten zur Verfügung stehen.

23. Erarbeitet in zwei Gruppen die gängigen Konzepte des Datenschutzes:

    Gruppe A erstellt das Konzept „Datenschutz durch Recht“.

    a) Welches Konzept liegt dem italienischen Datenschutzkodex zugrunde?
    b) Welches Konzept liegt den US-Datenschutzgesetzen zugrunde?

    Gruppe B beschäftigt sich mit dem „Datenschutz durch Technik“.

    a) Welche Techniken des Selbstschutzes gibt es? Welche Interessen werden durch Selbsthilfemaßnahmen geschützt?
    b) Was versteht man unter Datenschutz durch „Systemschutz“ und welche Interessen können dadurch geschützt werden?

5 Von der Medienkompetenz zum Mediendiskurs

Im Zentrum der Medienkompetenz steht die „digitale Selbständigkeit“. Der selbständige Nutzer handelt überlegt, weiß was er will, kann die neuen Medien bedienen, ist sich im Klaren, was er damit bewirkt, kennt alternative Wege, um digitale Projekte zu realisieren und wirft mitunter einen selbstkritischen Blick auf das eigene digitale Verhalten. Technische, ökonomische aber auch politische Entwicklungen der letzten Jahre machen deutlich, dass individuelle Medienkompetenz allein nicht ausreicht, das hohe Rechtsgut der Autonomie auch innerhalb der neuen Medien und Dienste zu gewährleisten.

5.1 Digitalisierung des Alltags

Die Digitalisierung des Alltags schreitet offenbar unaufhaltsam voran. PCs, Notebooks, Smartphones und das Internet sind allgegenwärtig. Das Internet ist multimedial und interaktiv geworden. In den 2000er Jahren sind neue Techniken des „Mitmachens“ entstanden. Nutzer informieren sich nicht nur im Netz und versenden E-Mails, sondern sie legen Wiki-Artikel an, laden Fotos auf Flickr hoch, offenbaren freimütig ihre Interessen auf sozialen Plattformen, betreiben einen eigenen Blog oder verfassen Kundenrezensionen zu Artikeln, die sie online erworben haben.

Die nächste Entwicklungsstufe des Internets, das „Internet der Dinge“, wird bereits eingeläutet. Mit dem Begriff wird ein Techniktrend beschrieben, bei dem PCs und Notebooks zusehends an Bedeutung verlieren und durch „intelligente Alltagsgegenstände“ ersetzt werden. Musste der Nutzer bei PCs per Maus und Tastatur Daten eingeben, erfolgt die Datenerfassung bei „intelligenten Dingen“ unmerklich im Hintergrund, ohne Wissen und Zustimmung der Nutzer. Ein paar Anwendungsbereiche sollen die neue Entwicklung illustrieren.

An erster Stelle steht das Smartphone als ständiger Begleiter, das die reale mit der virtuellen Welt über eine Vielzahl von Sensoren verbindet. Smartphones können beispielsweise mithilfe von GPS, WLAN, Bluetooth und Funkzellen Bewegungsdaten des Nutzers unbemerkt erfassen und an die Handyhersteller oder App-Anbieter senden. Solche Standortdaten lassen sich für lokalisierte Werbung vermarkten, wie etwa für Anzeigen eines Einkaufszentrums. Die Funktechnik Bluetooth ermöglicht den Vermarktern zu erfahren, an welchen Regalen im Einkaufszentrum der potentielle Kunde vorbeigeht, welche er aufsucht und bei welchen er wie lange verweilt. Mit Barcode-Scanner, den Shopping 2.0-Apps, kann der Kunde Testberichte zu elektronischen Geräten, Produktinfos zu Lebensmitteln, Infos zum Hersteller und Nutzerbewertungen abrufen sowie direkt den Preis

in den Geschäften der Umgebung, in Webshops oder bei eBay vergleichen. Verlangt die Barcode-App für ihre kostenlosen Dienste Telefonnummern, E-Mail-Adressen oder Informationen aus anderen installierten Apps abzurufen, gehen so weitere Daten „ins Netz“. Mikrofone und Kameras sind die „Ohren und Augen“ des Smartphones. Mit ihrer Hilfe können Gespräche samt Hintergrundgeräuschen aufgezeichnet oder Fotos geknipst werden. Richtet man die Handy-Kamera auf ein Bauwerk, erscheinen erklärende Informationen aus dem Web auf dem Handy-Display. Der Info-Anbieter weiß im Gegenzug, wo sich der Handy-Nutzer befindet und was ihn gerade interessiert.

Im Heimbereich ist es ein „intelligenter Rasensprinkler“, der selbständig entscheiden muss, ob der Rasen zu bewässern ist. Dafür nutzt der Rasensprinkler Daten von den Feuchtigkeitssensoren im Boden und Internetdaten zur Wettervorhersage. Der vielzierte smarte Kühlschrank warnt seinen Besitzer rechtzeitig, wenn Milch zur Neige geht oder das Verfallsdatum für die Joghurts naht und meldet Fehlfunktionen über das Internet an den Kundendienst. Für „überfürsorgliche“ Eltern gibt es bereits ein Armband für Kinder (KizON), das per App mit deren Smartphone verbunden ist. Kommt die Tochter nach dem Ballettunterricht nicht wie vereinbart nach Hause, können die Eltern mittels GPS-Daten ihren aktuellen Standort ermitteln.

Die Bekleidungsindustrie webt in den Stoffen „smart labels“ ein, in denen Produktinformationen, Kaufpreis sowie Gebrauchsanweisung enthalten sind. Mithilfe geeigneter Lesegeräte können solche Daten ausgelesen werden, etwa beim Bezahlen im kassenlosen Supermarkt oder in der Anprobe zum Abspielen individueller Videoclips zu Sonderangeboten.

Der Automobilsektor wird ebenso Teil des Internets der Dinge. GPS im Verbund mit Tachometer stellen beispielsweise Staus fest, Traktions-Sensoren erkennen Glatteis und melden dies den nachfolgenden Autos. Sensoren weisen den Halter auf Verschleiß und Reparaturnotwendigkeiten hin. Streikt der Motor unterwegs, sendet das Auto automatisch Diagnosedaten an den Pannendienst. Mit „Android Auto“ ist auch Google im Auto mit an Bord. Das ist eine Schnittstelle, mit der Android-Smartphones mit dem Infotainment-System des Autos per Bluetooth oder Kabel verbunden sind. Der Touchscreen im Auto dient als Bedienoberfläche für Android-Apps, die auf dem Smartphone laufen. Google-Server erhalten über das „Android Auto“ Informationen über das Fahrverhalten des Halters.

Schließlich gibt es eine Gruppe von Personen, bei der das Datensammeln Programm ist. Die Anhänger der sogenannten „Quantified-Self“-Bewegung protokollieren ihre Körperdaten. Fitness-Armbänder messen im Zusammenspiel mit Smartphone-Apps Puls, Schrittzahl, Höhenunterschiede oder Schlafpensum. Der Nutzer kann sich dann seinen Bewegungsradius auf Google Maps visualisieren lassen und erhält von Googles Werbekunden Vorschläge für sein künftiges Essverhalten. Google-Labor entwickelt eine elektronische Kontaktlinse für Dia-

betiker, die mithilfe eines Biosensors den Blutzuckerwert in der Tränenflüssigkeit messen kann. Ein Funkchip soll die Daten an eine begleitende Smartphone-App funken.[244]

Gefahren der allgegenwärtigen Datenverarbeitung: Der „digitalisierte Alltag“ birgt Risiken für die informationelle Selbstbestimmung. Die Kernprobleme dabei sind: die Datenerhebung erfolgt unbemerkt, der Nutzer weiß nicht, dass die installierte App Handydaten an App-Anbieter sendet; sie ist intransparent, der Nutzer erkennt nicht, welche Daten erfasst und weitergeleitet werden; die Datenerfassung wird ständig, rund um die Uhr, durchgeführt. Die Nutzer müssen keine Handlung durchführen, um ihre Daten preiszugeben, etwa sich ins Netz „einwählen“ oder ein Formular ausfüllen. Weiß der Nutzer nicht, wie Alltagsgegenstände per RFID-Chips miteinander kommunizieren und welche Daten sie in Echtzeit in Netz senden, kann er nicht rekonstruieren, was andere über ihn wissen und für welche Zwecke sie diese Daten verwenden. Kommerzielle Datensammler halten Daten auf Vorrat. Bahnt sich ein Geschäft mit Werbekunden an, wird klar, was mit den Daten passiert oder welche Daten mit welchen verknüpft werden sollen. Der Grundsatz der „informationellen Selbstbestimmung“ in der klassischen Ausprägung fordert hingegen, dass jeder rationale Datenentscheidungen trifft, weiß wer sie erhält und für welche Zwecke sie genutzt werden. Das „Internet der Dinge“ untergräbt die Datensouveränität der Bürger.

5.2 Netz-Ökonomie

Die vernetzte Ökonomie ist in erster Linie eine Datenökonomie. Online-Händler gehen von der Annahme aus, dass präzise Kundenprofile und individuelles Marketing ihren Umsatz steigern. Die Internet-Technologie bietet ihnen die Möglichkeit, aus den Datenspuren, die Kunden beispielsweise beim Online-Shopping hinterlassen, Kundenprofile zu erstellen und für gezielte Werbung zu vermarkten. Der Datenfluss, der beim Online-Shopping entsteht, ist beträchtlich. Schon bei der Produktsuche fallen verwertbare Daten an, denn der Web-Server erhält hierbei Informationen über Kundenpräferenzen. Bestellt der Kunde Waren, muss er seinen Namen, die Lieferanschrift und bei Kreditkartenzahlung auch die Kreditkarteninformationen angeben. Beim Online-Shopping entstehen Kundendaten nicht nur beim Online-Händler, sondern bei weiteren Akteuren: beim Service-Provider, der das Webangebot des Handlers bereitstellt; bei den Paketdiensten, welche für die Auslieferung der Ware sorgen und bei den Banken, über welche die Bezahlung abgewickelt wird. Verwertbare

244 Ist die nächste Stufe des „Internet der Dinge“ der netzfähige „Maschinenmensch“? Im Roman „Maschinenmann“ erzählt der Autor Max Barry wie ein Ingenieur ein Bein durch eine Prothese ersetzt. Als der Ingenieur feststellt, dass seine Prothese leistungsfähiger ist als sein altes Bein, geht er daran peu à peu das zweite Bein, die Hände, die Augen zu ersetzen. Der Roman wirft eine ernsthafte moralische Frage auf. Wo liegen die Grenzen der technischen Machbarkeit? Ist das Streben nach körperlicher Perfektion Ausdruck individueller Autonomie? Wie wirkt sich ein „Internet der Körperteile“ auf die Autonomie der Menschen aus?

Daten fallen auch beim einfachen Surfen an. Web-Server beobachten per Cookies und Tracker, was den Nutzer im Netz interessiert, welche Angebote er wiederholt aufruft oder zu welchen Artikeln er nach Zusatzinformationen sucht. Erfahren Werber etwa, dass eine Frau schwanger ist, ist das für sie eine Power-Konsumentin. Mit entsprechender Werbung ist da in nächster Zeit für Eltern-Ratgeber, Windeln, Babynahrung, Kinderspielzeug oder Kinderwagen viel Geld zu machen.

> *„Es (das Web) muss ein offenes, neutrales und dezentralisiertes Netzwerk bleiben, in dem Menschen rund um den Planeten zusammen an Innovationen arbeiten."*
>
> Tim Berners-Lee, Erfinder des World Wide Web

Die vernetzte Ökonomie ist auch ein Markt für neue Monopole. US-Unternehmen haben in den 2000er Jahren im globalen Wettbewerb ein Geschäftsmodell durchgesetzt, das nun im Zentrum der vernetzten Ökonomie steht. Der Informatiker Jaron Lanier nennt die IT-Player wie Google, Facebook & Co. „Sirenenserver".[245] Die Dienste, die sie anbieten, kosten dem Nutzer nichts. Google bietet neben der Suchmaschine eine ganze Palette von Gratisdiensten an[246], die zweifelsohne das Leben im Netz erleichtern. Zum Symbol für Gratisdienste ist auch Facebook geworden. Die Nutzer können Inhalte kostenlos „teilen" und „liken". Finanziert werden die Gratisofferten durch Werbung. Facebook & Co. liefern große Nutzerzahlen und Informationen über die Nutzer und die Werbekunden zahlen dafür, dass sie passgenau Werbemaßnahmen, wie Banner, Laufschriften, Werbelinks oder Videoclips schalten können.[247]

Gefahren der Netz-Ökonomie: Die Netz-Ökonomie verschärft die Fragen nach dem autonomen Leben im digitalisierten Umfeld. Werden Daten, die von kommunikationsfähigen Alltagsgegenständen ausgehen, zusammengeführt, kann ein detailliertes Bild über Interessen, Neigungen, Tagesverlauf oder Gemütszustand des Besitzers erstellt werden. Diese Informationen können Vermarkter dazu nutzen, gezielt Anreize zu platzieren, um den Betroffenen in seinem Kaufverhalten zu beeinflussen. Der Betroffene ist sich nicht bewusst, dass er genau jene Kaufangebote erhält, die bei ihm einen Kaufreiz auslösen. Der Konsument ist nicht in der Lage, sämtliche Kosten, Nutzen und Alternativen zu überschauen, wohlüberlegt zwischen diesen abzuwägen

245 Jaron Lanier (2014): *Wem gehört die Zukunft. Du bist nicht der Kunde der Internet-Konzerne, du bist ihr Produkt,* Hamburg. Sirenen sind in der griechischen Mythologie weibliche Fabelwesen, die auf Klippenfelsen wohnten, mit ihren betörenden Gesängen Seemänner anlockten, um sie zu töten und zu verspeisen. Odysseus, der berühmteste griechische Seefahrer, wurde rechtzeitig vor den Sirenen gewarnt und bat seine Matrosen ihre Ohren mit Wachs zu verschließen und ihn selbst an den Schiffsmast zu binden. So konnte Odysseus ihren Gesang hören und zugleich mit Vernunft seine Haut retten.

246 http://www.google.de/about/products/

247 Lanier's Antwort auf die Gratiskultur ist das Modell der „humanistischen Informationsökonomie". Danach sollten Google, Facebook & Co. für jede Information, die deren Nutzer preisgeben, über eine Art Mikrobezahlsystem bezahlen. Das Modell der „humanistischen Informationsökonomie" ist nicht wirklich überzeugend, weil dadurch porentief bzw. Bit für Bit sämtliche Bereiche der digitalen Privatsphäre und des sozialen Austausches von der „Logik des Marktes" beherrscht würden. „Digitale Selbständigkeit" wäre nur eine Scheinselbständigkeit. Jedenfalls gibt es schon erste Geschäftsmodelle für den Direktverkauf von Personendaten. Citizen.Me (http://www.citizenme.com/) hat eine App entwickelt, mit deren Hilfe Nutzer ihre persönlichen Daten direkt an Daten-Broker verkaufen können. Werber erhalten bessere Informationen und Nutzer können so die eigenen Daten an den Meistbietenden verkaufen.

und handelt deshalb zu Lasten des eigenen Wohls nur eingeschränkt rational.

Zum Begriff der Freiheit gehört auch die Willensfreiheit. Diese liegt vor, wenn Personen die Urheber ihrer Handlungen sind. Ist der Kaufwille nicht mehr Ausdruck eines informierten und reflektierten Willens, steht die Konsumentensouveränität auf dem Spiel. Grundlage der Nachfrage bilden nicht mehr die reflektierten Bedürfnisse, sondern die durch gezieltes und allgegenwärtiges Marketing überformten Bedürfnisse. Die neuen Medien im Verbund mit den Geschäftsmodellen der Internetkonzerne dominieren zusehends die Lebenswelt der Menschen.

5.3 NSA & Co. im Netz

Im Juni 2013 begann die Geschichte des NSA-Skandals. Der britische Guardian und die amerikanische Washington Post begannen geheime Dokumente zu veröffentlichen, die sie vom ehemaligen NSA-Mitarbeiter Edward Snowden erhalten hatten. Snowden floh nach Russland ins Exil. Die Dokumente brachten ein weltweites Spionagesystem im Internet ans Tageslicht. NSA & Co. können offenbar alles machen, was technisch möglich ist.

Wer wird überwacht? Neben transnationalen terroristischen Netzwerken weltweit Regierungschefs und Regierungspersonal, EU-Institutionen, die Zentrale der Vereinten Nationen, Telekommunikationsanbieter und alle US-Bürger. Werden alle Menschen weltweit überwacht? Offenbar sind NSA & Co. in der Lage, das Internet umfassend zu scannen. „Man braucht den Heuhaufen, um darin die Nadel zu finden“, so der ehemalige NSA-Direktor Keith Alexander. Was heißt Scannen? Dabei wird die Internetkommunikation nach Anhaltspunkten durchforstet, ob sie von Terroristen stammen könnte. Gibt es hierzu Anzeichen,[248] sehen sich Analysten den Datenverkehr genauer an. Am Ende wird die Liste für eine gezielte Observation erstellt.

Wie erfolgt die Überwachung? Um an die Daten zu kommen, zapfen NSA & Co. mit Tempora See- und Glasfaserkabel an, kooperieren mit US-Internetprovidern,[249] greifen mit Prism auf Nutzerdaten von IT-Playern, wie Facebook, Google & Co. zu, fangen Postsendungen ab und bauen Hintertüren in die IT-Hardware, wie Router ein, bevor sie zum eigentlichen Adressaten weitergeleitet werden, spähen mit Hacienda per Portscan ver-

248 Die Anzeichen gehen nicht aus den Daten selbst hervor, sondern ergeben sich erst aus der Verbindung der Daten mit definierten Merkmalen. Damit stellt sich die rechtsstaatliche Frage, nach welchen Merkmalen die Liste der „Terrorverdächtigen“ erstellt wird: http://sz.de/1.2061380; http://sz.de/1.2078869. Offenbar geraten auch jene Personen ins Visier der US-Geheimdienste, die sich digitaler Hilfen, wie der Anonymisierungssoftware Tor, bedienen: http://www.tagesschau.de/inland/nsa-xkeyscore-100.html

249 IT-Firmen mit Sitz in den USA unterliegen dem US-Recht. Die National Security Letters (dt. Nationaler Sicherheitsbrief) sehen vor, dass US-Behörden Zugriff auf Nutzerdaten oder Crypto-Programme verlangen und zugleich anordnen können, nicht über den Erhalt oder deren Inhalt zu sprechen.

wundbare Netze aus und kartieren sie, schwächen Kryptographie-Software, lesen Smartphone-Daten, wie Standortdaten, Gerätenummer des Handys (IMEI), SIM-Kartennummer (IMSI), SMS, Chats, E-Mails, Surfdaten aus oder schneiden Skype-Gespräche in Echtzeit mit. Die NSA-Vision: Mobile Geräte, Rechner und Netze jederzeit ausspionieren, kapern und Angriffe verschleiern zu können.

> *„Jeder Mensch hat drei Leben: ein öffentliches, ein privates und ein geheimes."*
>
> Gabriel García Márquez, Literaturnobelpreisträger

Wozu die globale Überwachung? Erstens, um Terroranschläge wie die von 9/11 zu verhindern. Dafür braucht es rechtzeitige Informationen über transnationale terroristische Netzwerke, ihre Anschlagspläne, Rekrutierungen und Finanzströme. Zweitens, um die tatsächlichen Ziele und Pläne der Sicherheits- und Außenpolitik autoritärer und totalitärer Staaten auszuforschen. Die Ausspähung von Regierungschefs befreundeter demokratischer Staaten, der Vereinten Nationen oder der EU-Institutionen hat allerdings nichts mit der Verfolgung terroristischer Aktivitäten im Internet zu tun. Drittens, gehört auch die Wirtschaftsspionage zum Kerngeschäft der Auslandsaufklärung? Um Rüstungsfirmen auszuspionieren, die illegal Militärgerät in Krisengebiete verkaufen und damit die regionale Sicherheitslage verschärfen oder Firmen, die sicherheitsrelevante Technik oder Software entwickeln? Werden die Dienste für das „wirtschaftliche Wohlergehen" ihrer Länder eingesetzt, etwa indem sie Know-how von Firmen abfischen, verschaffen sie ihnen einen unlauteren Wettbewerbsvorteil und verstoßen gegen Prinzipien des freien Marktes.

Gefahren der NSA-Überwachung: NSA & Co. haben im Netz Aktivitäten ergriffen, die kritisch zu hinterfragen sind. Die präventive, anlasslose Massenüberwachung der digitalen Kommunikation verletzt das Grundrecht auf unversehrte Kommunikation. Massenüberwachung verletzt die freie Persönlichkeitsentfaltung und beschädigt die Demokratie. Die vertrauliche Kommunikation ist gewissermaßen das Gewächshaus für die individuelle Persönlichkeitsentfaltung und die freie Debatte ist Voraussetzung für eine funktionierende Demokratie.

Ist die globale Überwachung ein „Big Brother"? George Orwell beschreibt im Roman „1984" einen totalitären Staat, indem die Freiheitsrechte eingeschränkt werden. Jedes Zimmer ist mit Mikrofonen und sog. Televisoren ausgestattet, die nicht abgeschaltet werden können und die Bürger überwachen, um zu gewährleisten, dass sie regierungskonform reden und handeln. Unstrittig ist, dass NSA & Co. nicht Teil eines „Big Brother" sind. Freie Meinungsäußerung, Pressefreiheit[250] und politischer Pluralismus zählen zum Markenkern

250 Die Menschenrechtsorganisation Human Rights Watch (HRW) berichtet in einer Studie, dass die massive NSA-Überwachung auch die Arbeit der investigativen Journalisten in den USA erschwert: http://www.hrw.org/node/127364. Aufgabe des investigativen Journalismus ist durch akribische und verdeckte Recherchen Missstände in Staat, Wirtschaft und Gesellschaft der Öffentlichkeit bekannt zu machen. Eine freie Presse, als „vierte Gewalt" im Staat, stellt für die Bürger eine unverzichtbare Informationsquelle für eine fundierte politische Urteilsbildung dar.

der US-Verfassung. Bürger mit politisch abweichenden Meinungen und oppositionelle Gruppen dürfen weder identifiziert noch politisch verfolgt werden.[251]

Ist die globale Überwachung ein digitales Panopticon? Das Panopticon war im späten 18. Jahrhundert ein Entwurf von Jeremy Bentham für Gefängnisbauten. Es besteht aus einem kreisförmigen Gebäude, das um einen Wachturm in der Mitte angeordnet ist. Die Insassen der Zellen können die Wächter im Turm nicht sehen während sie selbst jederzeit beobachtet werden können. Da der Insasse jederzeit davon ausgehen muss, dass ein Aufseher tatsächlich auf ihn blickt, passt er sein Verhalten den Gefängnisregeln an. Ein digitales Panopticon ist mit einer freien Gesellschaft unvereinbar. Die Furcht vor Überwachung hemmt die Bürger frei zu reden, abweichende Meinungen zu vertreten oder sich an regierungskritischen Aktivitäten zu beteiligen. Die Metapher vom Panopticon hinkt. Die Bürger freier Demokratien konsumieren gewissermaßen die Überwachung, sie sitzen nicht isoliert in einer Zelle. Die neuen Monopole mit ihren Gratisangeboten, Apps und Geräten bieten Annehmlichkeiten, Hilfen für den Alltag und entlasten den Nutzer von Routineaufgaben. Vieles rechnet sich nur, weil die neuen Monopole das Internetverhalten der Nutzer tracken und die Datenspuren vermarkten.

Die massenhafte Überwachung ist der Abschied vom Rechtsstaat so wie wir ihn kennen. Überwachung darf im Rechtsstaat nur in den Fällen erfolgen, die das Gesetz zur Gewährleistung von Sicherheit vorsieht und die transparent und gerichtlich kontrollierbar sind.[252] Der Gedanke des Generalverdachts ist dem Rechtsstaat fremd. Im Präventionsstaat hingegen gilt die Devise: „Jeder Bürger ist ein potenzieller Terrorist.“ Der Staat hat dann nicht nur die Aufgabe Schaden abzuwehren, sondern der Entstehung von Schäden durch vorausschauende Interventionen vorzubeugen. Im Rechtsstaat kann der gesetzestreue Bürger darauf vertrauen, vom Staat in Ruhe gelassen zu werden. Im Präventionsstaat erweckt gerade die unauffällige Lebensweise den Verdacht ein „Schläfer“ zu sein. Nimmt der Staat die politische Gesinnung der „Risikogruppen“ ins Visier, wird das Verfassungsgebot der Gleichbehandlung untergraben. Prävention beruht auf dem Erwerb von umfassenden Informationen. Die Sicherheitsbehörden müssen bereits im Vorfeld in Erfahrung bringen, in welchem gesellschaftlichen Milieu Gedanken für terroristische Anschläge keimen könnten. Die massenhafte Überwachung der Internetkommunikation ist dann nur folgerichtig. Die Suspendierung des demokratischen Rechtsstaates, der „Ausnahmezustand“ ist keine Ausnahme mehr, so der Philosoph Giorgio Agamben, sondern wird immer mehr das „herrschende Paradigma des Regierens.“[253] Der Ausnahmezustand als Regel hält einem Fakten-

251 Das Gefangenenlager Guantánamo, ein Stützpunkt der US-Navy auf Kuba, verletzt offen das Rechtsstaatsprinzip. Seit Jahren werden dort „feindliche Kämpfer“ festgehalten, ohne Anklage und ohne ordentliches Gerichtsverfahren. Im Prinzip kann jeder ins Visier der Dienste geraten, wenn per digitaler Rasterfahndung aus ein paar Einzelindizien ein unbegründeter Anfangsverdacht hervorgeht. Vgl. *„Taxi zur Hölle“* (2010), Alex Gibney, ARD, 21.10.2010, 20:15 Uhr.

252 Das „Recht auf Sicherheit“ nach Art. 5 EMRK ist ein Recht der Bürger vor staatlicher Willkür.

253 Giorgio Agamben (2004): *Ausnahmezustand,* Frankfurt a. M., S. 9, 102; (2014): *Die Geburt des Sicherheitsstaats,* Le Monde diplomatique Nr. 10360, 14.3.2014, http://www.monde-diplomatique.de/pm/2014/03/14.mondeText.artikel,a0065.idx,12

check allerdings nicht stand. Der schleichende Übergang vom Rechtsstaat zum Präventionsstaat erfolgt in freiheitlichen Demokratien nicht per Autopilot. Grundfreiheiten stellen sicher, dass politische Entwicklungen stets offen bleiben. Rechtsbrüche können auf Druck einer empörten Öffentlichkeit jederzeit revidiert werden.

5.4 Web 2.0-Diskurs

Die Entwicklung der neuen Medien, das Web 2.0, ermöglicht insbesondere der Zivilgesellschaft sich öffentlich zu äußern. Jeder kann zum Autor werden, einen eigenen Blog betreiben, Beiträge anderer kommentieren, ein Podcast anbieten oder einen neuen Thread in einem Forum eröffnen. Netzaktivisten, Datenschützer, Bürgerrechtler oder Crypto-Experten können gleichberechtigt ihre Standpunkte und Argumente vortragen, etwa die Datenschutzpolitik der EU analysieren, Nutzen und Gefahren von Crypto-Apps gegeneinander abwägen oder zu einer Petition an Gesetzgeber aufrufen. Das vernetzte Kollektiv überprüft, bestätigt oder stellt in Frage. Bestand hat, was die (rationale) Netzwerkgesellschaft akzeptiert. Ein erfolgreiches Beispiel für die „Weisheit der Vielen“ ist Wikipedia.

Datenschutz-Syllogismus

- Obersatz (O): Alle Menschen (M) haben ein Grundrecht auf informationelle Selbstbestimmung (S).
- Untersatz (U): Bestimmte IT-Infrastrukturen (T) sind notwendige Bedingungen für die Ermöglichung des Grundrechts auf informationelle Selbstbestimmung (S).
- Konklusion (K): T müssen zur Ermöglichung von S gewährleistet werden.

Was kann ein Web 2.0-Diskurs im Hinblick auf die Netz-Gefahren leisten? Aufklärung und Klarheit, wie beispielsweise die „informationelle Selbstbestimmung“ in einem Umfeld, wo die digitale und reale Welt miteinander verschmelzen, neu definiert werden muss. Ist Datenschutz ein Kampf gegen Windmühlen? Könnten sogenannte Datenschutz-Apps auf Smartphones dem Nutzer helfen, unkompliziert seine Datenschutzpräferenz umzusetzen? Ist der Datenschutzansatz „Privacy by Default“ mit den kommerziellen Interessen von Seitenbetreibern und Herstellern netzwerkfähiger Endgeräte vereinbar?[254] Muss ein effektiver Datenschutz verstärkt auf Schutz durch Technik setzen? Sollte der Datenschutz bereits von Anfang an in die Technik eingebaut sein, sodass nur solche Daten abgefragt werden können, die abgefragt werden dürfen? Datenschützer sprechen von „Privacy by Design“. Wie schützt die Regierung die Bürger vor Bespitzelung durch NSA und andere Dienste? Warum sollte die Politik aus Sicherheitsgründen Open-Source-Software oder Freie Software fördern? „Die

254 Das Android-Smartphone Blackphone ist ein Beispiel für das Konzept „Privacy by Default“. Mit dem Blackphone sollen E-Mails, Chats, Apps und Daten abhörsicher sein: https://www.blackphone.ch

Republik“, so die italienische Verfassung, „anerkennt“ die unverletzlichen Rechte des Menschen nicht nur, sondern „gewährleistet“ sie auch (Art. 2 Verf.).

Hat die digitale Öffentlichkeit Einfluss auf die demokratische Willensbildung? Die digitale Öffentlichkeit ermöglicht jedenfalls der Netzwerkgesellschaft den politischen Prozess kritisch zu begleiten. Der tatsächliche Einfluss hängt davon ab, ob Netzaktivisten ein Thema setzen können, die Netzwerkgesellschaft das Thema aufgreift, aufbereitet und verstärkt, die vielen Beiträge zu politischen Forderungen bündelt, die traditionellen Medien darüber berichten und ob sie schließlich für ihre Forderungen Bündnispartner in der realen Welt findet.

> *„Wer in Freiheit leben will (…) muss lernen, mit Unsicherheit zu leben und mit Angst gelassen umzugehen.“*
>
> Johano Strasser, Politologe und Schriftsteller

Der Web 2.0-Diskurs setzt eine aufgeklärte Gesellschaft voraus, die im Alltag überlegt digitale Technologien einsetzt. Das Fatale ist, dass die Ideenökonomie sich so schnell entwickelt und Innovationen in kürzester Zeit marktfähig sind, dass fürs gründliche, sachkundige Überlegen, Abwägen und Diskutieren keine Zeit bleibt. Ein effektiver Mediendiskurs ist offen, dezentral und kontrovers. Kein Diskurs liegt vor, wenn Mitglieder eines Forums politisch eine homogene Gruppe bilden, Beiträge lediglich „liken“ oder ohne Gründe und Sachkenntnis kommentieren.

Die Logik der Geheimdienste: „Um wirklich sicher zu sein, muss man alles wissen“ und die Logik der Internetkonzerne: „Je mehr Informationen über den Kunden umso besser fürs Geschäft“ kann durch aufgeklärte Mediendiskurse aufgebrochen werden. Es liegt letztlich beim Gesetzgeber, den Ordnungsrahmen für die Netz-Ökonomie festzulegen und sich mehr für den digitalen Freiheitsstaat oder mehr für den Sicherheitsstaat zu entscheiden. Die öffentliche Debatte der Zivilgesellschaft kann der Politik Legitimität verschaffen oder entziehen, die dann mitunter auch eine Kurskorrektur der Politik zur Folge haben kann. Die „Schwarmintelligenz“ kann hierfür das erforderliche Orientierungswissen bereitstellen. Medienkompetenz stellt sicher, dass die Netzwerkgesellschaft handlungskompetent argumentiert.

Glossar/Abkürzungen

Abmahnung: außergerichtliches Schreiben an eine Person, in dem steht, dass sie gegen ein Recht verstoßen hat, verbunden mit der Aufforderung, den Verstoß in Zukunft zu unterlassen, z. B. umgehend ein widerrechtlich verwendetes Bildnis von einer Webseite zu nehmen.

Abstract: kurze Inhaltsangabe einer wissenschaftlichen Publikation

Access-Provider: bietet den Zugang zum Internet an.

Administrator: eine Person, deren Aufgabe es ist, Server, PCs und Netzwerke betriebsbereit zu halten und für die Sicherheit der Daten zu sorgen. Bei Facebook handelt es sich hierbei um Personen, die eine Gruppe oder Fanpage gründen und verwalten.

AdWords: Google’s Suchmaschinen-Werbung. Hierbei erscheinen Textanzeigen neben den Suchergebnissen unter der Spaltenüberschrift „Anzeigen“ bzw. farblich hervorgehoben über den Suchergebnissen unter „gesponserte Ergebnisse“. Die Textanzeigen werden eingeblendet, wenn sie zum Inhalt der Suchanfrage passen.

AdSense: Google’s Werbe-Partnerprogramm, bei dem Werbeanzeigen eingeblendet werden, die zum Inhalt der Webseiten passen.

Alert: Benachrichtigung, dass Informationen aktualisiert wurden, etwa dass die aktuelle Ausgabe einer Monatszeitschrift nun online abrufbar ist oder dass die Literatursammlung einen neuen Eintrag erhalten hat.

APK: (Abk. für Android Application Package Files) Installationsdatei einer App, so wie unter Windows die .exe-Datei. Die .apk-Datei ist eine gepackte Datei, in der mehrere Ordner enthalten sind.

Aktivitätsprotokoll: hier sieht man in chronologischer Ansicht alle Statusmeldungen einer Person, alle Kommentare unter den Beiträgen von Freunden, alle gelikten Online-Inhalte oder mit wem man eine Freundschaft eingegangen ist.

Apps: (Abk. für Applications) bezeichnet zusätzliche Anwendungen, welche man auf Facebook und Smartphones installieren und nutzen kann. Für das iPhone von Apple kann man Apps im „AppStore“ aussuchen, für das Android von Google im „Google Play Store“.

Assistent: Computerprogramm, das dem Nutzer bestimmte Informationsarbeiten abnimmt und ihm ein virtueller Gehilfe ist. So gibt es eine Vielzahl von Assistenten, vom Installations-, Update-, Such- bis hin zum Filterassistenten, die unerwünschte Werbung blockieren.

Authentizität: Grundwert der IT-Sicherheit und bedeutet, dass beispielsweise E-Mail-Nachrichten zweifelsfrei einem eindeutigen Absender zugeordnet werden können.

Backdoor: (dt. Hintertür) Hintertür in einer Software, die es Angreifern ermöglicht, unberechtigte Zugriffe über das Internet auf fremde Betriebssysteme, Programme und Datenbestände zu erlangen.

Backlink: (dt. Rückverweis) eingehender Link auf eine Webseite. Suchmaschinen verwenden die Anzahl der Backlinks auch als Maßstab für die Linkpopularität einer Webseite.

Bestandsdaten: dazu zählen insbesondere Name und Anschrift des Vertragspartners. Bestandsdaten sind erforderlich, um Verträge mit bestimmten Personen zu begründen, abzuändern oder zu beenden.

Bibliothekskatalog: Verzeichnis von Publikationen wie Büchern, E-Books oder Zeitschriften, die in einer oder mehreren Bibliotheken vorhanden sind und auch über den Standort der Publikation in der Bibliothek informieren.

Bibliografie: Verzeichnis, das die Publikationen zu einem bestimmten Thema auflistet.

Big Data: großer Datenhaufen; Firmen, Behörden und Wissenschaftler sammeln und werten große Datenmengen aus, für neue Geschäftsmodelle, für effizientere öffentliche Leistungen und für neue Erkenntnisse. Mit Big Data kann man menschliches Verhalten besser vorhersagen und kontrollieren.

Bloatware: vorinstallierte Apps bei Smartphones. Solche unerwünschten Apps lassen sich mitunter schwer entfernen.

Bluetooth: Funkstandard für Datenkommunikation. Mittels Bluetooth kann z. B. eine MP3-Datei vom PC auf das Smartphone übertragen werden.

Botnetz: Verbund von meist mehreren Tausend PCs oder Smartphones, der unter der Kontrolle eines Angreifers steht und dazu missbraucht wird, per Fernsteuerung beispielsweise das Internet mit Spams zu überfluten oder Angriffe auf Webserver durchzuführen.

Boolsche Operatoren: bei Recherchen in Suchmaschinen ermöglichen sie die Verknüpfung oder den Ausschluss von Suchbegriffen, wie z. B. AND („und“), OR („oder“) und NOT („nicht“).

c.c.: codice civile, Zivilgesetzbuch

CC-Lizenz: (Abk. für Creative Commons-Lizenz) modular aufgebautes Lizenzmodell, das eine Alternative zum klassischen Urheberrecht darstellt. Der Urheber legt fest, was der Nutzer mit dem Werk machen darf und was nicht (https://creativecommons.org/licenses/by-nc-nd/3.0/deed.de).

CDDB: (Abk. für Compact Disc Database) Datenbanken, die Metadaten (Interpret, Album, Titel, Jahr, Genre) über die auf dem Markt befindlichen Audio-CDs enthalten. Die Tags können über das Internet abgerufen werden.

Chat: Kommunikation in Echtzeit über das Internet, die per Text, Audio oder Video erfolgen kann.

Client: Soft- oder Hardware, die auf Dienste eines Servers zugreift, um Anwendungen oder Dateien nutzen zu können. Man spricht auch von Kunde oder „Anfrager“.

Cloud: (dt. Datenwolke) ein virtueller Speicherraum, in dem Daten gesichert und mit mehreren Nutzern, die über eine entsprechende Berechtigung verfügen, geteilt werden können.

Containerdatei: Datei, die andere Datentypen, wie Text, Audio, Videos, Fotos oder PDFs enthält.

Content-Provider: stellt Inhalte (engl. Content) wie Texte, Fotos, Software u.v.a.m. für die User zur Verfügung.

Cookie: (dt. Keks) Textdatei, die auf Anweisung des Web-Servers beim Surfen auf den PC gespeichert wird. Sie kann Daten darüber enthalten, welche Webseite ein Nutzer wie häufig und wie lange aufruft, welche Waren dieser in den Warenkorb abgelegt hat, welchen Browser oder welches Betriebssystem er nutzt.

Copyleft-Lizenz: Urheber dürfen fremde Werke nur dann bearbeiten und verbreiten, wenn sie das „abgeleitete Werk“, z. B. die ursprüngliche Software mit zusätzlichen Funktionen, unter derselben Lizenz verbreiten.

Cover: Neueinspielung eines Musiktitels durch einen anderen Interpreten

c.p.: codice penale, Strafgesetzbuch

c.p.p.: codice di procedura penale, Strafprozessordnung

Crowdfunding: Medieninhalte werden erst produziert, sobald das Geld zu ihrer Herstellung beschafft wurde. Finanziert werden die Inhalte über Onlineportale durch die Internetnutzer, weshalb man auch von einer Schwarmfinanzierung spricht.

Crowdsourcing: lagert Aufgaben an Internetnutzer aus, die freiwillig und kooperativ für ein bestimmtes Projekt Leistungen erbringen. Croudsourcing setzt auf die „Weisheit der Massen“, mit deren Hilfe kostengünstigere, bessere und innovativere Leistungen erzielt werden sollen.

Custom Rom: alternatives zum vorinstallierten Android-Betriebssystem, das in der Regel nicht vom Geräteherstellers selbst stammt, sondern von Teams aus Freiwilligen entwickelt und laufend aktualisiert wird.

Deskriptor: Stichwort, das den Inhalt eines Dokuments oder einer Information charakterisiert.

Desktop-Suchmaschine: Programm, das Text-, Bild-, Musik- oder Video-Dateien indexiert und mit dessen Hilfe Dateien auf dem eigenen PC gesucht werden können.

Digitale Signatur: digitales Gegenstück zur handschriftlichen Unterschrift auf Papier. Sie wird mithilfe eines kryptographischen Verfahrens erzeugt und dient dazu, den Absender einer Nachricht zweifelsfrei zu identifizieren und sicherzustellen, dass die Nachricht auf dem Weg zum Empfänger nicht verändert wurde.

Digitales Zertifikat: „digitale Identitätskarte“, die von einer autorisierten Zertifizierungsstelle digital beglaubigt wird. In der Regel enthalten digitale Zertifikate den Namen des Inhabers und Ausstellers, die Gültigkeitsdauer und den Verwendungszweck. Digitale Zertifikate stellen sicher, dass die damit signierten Dokumente zweifelsfrei von der angeführten Person stammen, verschlüsselt im Netz übertragen werden und nicht manipuliert werden können.

D.L.: decreto legge, Notverordnung

D.lgs.: decreto legislativo, Ermächtigungsverordnung

Domain: Internetadresse, unter der Nutzer eine Webseite erreichen. Mithilfe der Domain kann man auch feststellen, wer inhaltlich für die bereitgestellten Informationen verantwortlich ist.

dpi: (Abk. für dots per inch) gibt an, wie viele Bildpunkte pro Zoll (ca. 2,5 cm) abgebildet werden. Je mehr Bildpunkte pro Zoll, desto höher ist die Auflösung eines Druckers, Scanners oder Monitors.

DRM: (Abk. für Digital Rights Management) digitales Rechtemanagement. Es bezeichnet technische Verfahren, die dazu dienen, das Kopieren geschützter Werke zu blockieren oder ihre Nutzung einzuschränken.

Dynamische Webseite: Webinhalte, die erst auf Anfragen des Nutzers individuell erzeugt werden, wie bei großen Online-Shops oder eBay.

E-Book: (dt. elektronisches Buch): Buch in digitaler Form, das Texte, Bilder sowie multimediale Inhalte und Hyperlinks enthalten kann. Zum Lesen benötigt der Nutzer spezielle Wiedergabegeräte wie E-Book-Reader oder Lesesoftware auf PCs, Notebooks oder Smartphones.

EMRK: Europäische Menschenrechtskonvention

Ende-zu-Ende-Verschlüsselung: ein Verfahren der Verschlüsselung, bei dem die Nachricht bereits auf dem PC (oder Smartphone) des Absenders verschlüsselt und erst beim Empfänger entschlüsselt wird. Auf dem gesamten Weg vom Absender zum Sender bleibt die Nachricht gegen Zugriffe geschützt, weder der Anbieter der Verschlüsselungssoftware noch Behörden oder Werbefirmen haben auf die gesendeten Informationen Zugriff.

Enzyklopädie: Nachschlagewerk, das in alphabetischer Reihenfolge Artikel zu einem bestimmten Thema enthält und dem Nutzer erlaubt, sich schnell einen einführenden Überblick über ein Thema zu verschaffen.

Erschöpfungsgrundsatz: ein Werkträger (CD mit Musik, CD-Rom mit Software), der rechtmäßig im EU-Raum auf den Markt gebracht wurde, darf frei weiterverkauft werden.

EuGH: Europäischer Gerichtshof

Eula: (Abk. für End User Licence Agreement) Endbenutzer-Lizenzvertrag, der regelt, was der Nutzer mit einer Software machen darf und was nicht erlaubt ist.

Exif: (Abk. für Exchangeable Image File Format) Standardformat für das Abspeichern von Aufnahmeinformationen in Fotos, wie Aufnahmedatum, Belichtungszeit, Blende, ISO-Wert oder Kamerahersteller.

Fake: (dt. Fälschung, Betrug) Das kann ein gefälschtes Facebook-Profil, eine E-Mail mit falschem Absender oder ein gefälschter Username in einem Forum sein. Fakes dienen dazu, die tatsächliche Identität einer Person zu verschleiern.

Filesharing: siehe Tauschbörse

Fingerabruck: (engl. fingerprint) eine Zeichenkette aus Zahlen und Buchstaben von einer bestimmten Länge. Beim MD5-Verfahren sind es 32, beim SHA1 40 und beim SHA512 128 Zeichen. Der Fingerabdruck wird verwendet, um etwa die Korrektheit des öffentlichen Schlüssels bei der E-Mail-Verschlüsselung nachzuweisen.[255]

255 Mit der Software DP Hash (http://www.paehl.de/cms/hash_dp_deutsch) kannst du den Fingerabdruck von Dateien erstellen und überprüfen.

Frame: (dt. Rahmen) Teilbereich des Browser-Fensters, der mit verschiedenen Inhalten gefüllt werden kann, wie Inhalts- und Navigationsbereich. Die Inhalte der Frames können auf anderen Servern liegen und erst beim Aufruf der Webseite oder bei Abfrage bestimmter Inhalte in die Webseite integriert werden.

Freeware: Software, die Nutzer privat kostenlos nutzen dürfen. Manche Freeware-Lizenzen sehen auch vor, dass die Software verbreitet und kommerziell genutzt werden kann. In der Regel darf der Programmcode von Freeware nicht weiterentwickelt werden.

Freie Software: Software, deren Quellcode einsehbar ist, die man beliebig verwenden, anpassen, in eigene Programme integrieren, kopieren, verändern und wieder in den Umlauf bringen kann. Freie Software wird als emanzipatorische Technologie verstanden, die eine Alternative zur proprietären Software bildet.

Filehoster: stellt im Internet Speicherplatz zur Verfügung. Der Nutzer kann ohne Registrierung und mit einem Klick, beispielsweise Fotos oder Videoclips, auf die Seite des Filehosters hochladen. Im Gegenzug erhält er einen Downloadlink, mit dem er die hochgeladene Datei jederzeit wieder abrufen kann.

Firewall: (dt. Brandmauer) schützt PCs oder Smartphones vor unbefugtem Datenverkehr mit dem Internet.

Forensik: fasst berufliche Tätigkeiten zusammen, die sich im Rahmen eines Gerichtsverfahrens damit befassen, kriminelle Handlungen zu identifizieren, zu analysieren und zu rekonstruieren.

Garante Privacy: (Garante per la protezione dei dati personali) italienische Datenschutzbehörde

GCHQ: (Abk. für Government Communications Headquarters) britischer Geheimdienst

„Gefällt-mir“-Button: damit kann ein Facebook-Nutzer Texte, Fotos, Videos, Musik oder Artikel überall im Netz seinen Facebook-Freunden empfehlen. Im Gegenzug weiß Facebook, welche Webseiten ihre Mitglieder aufgerufen haben und kann somit gezielter Werbung schalten.

GIF: (Abk. für Graphics Interchange Format) Bildformat im Internet, das maximal 256 Farben darstellen kann. Es eignet sich besonders für Logos oder Cliparts.

GNU FDL: (Abk. für GNU Free Documentations License; GNU Freie Dokumentationslizenz) Lizenz für freie Inhalte. Sie erlaubt, Texte frei zu vervielfältigen, gewerblich zu nutzen oder auch zu bearbeiten, sofern die abgeleiteten Texte ebenso frei weitergegeben werden.

GNU General Public License: (GPL) Softwarelizenz, die Nutzern erlaubt, die Software zu nutzen, zu kopieren, zu verbreiten, anzupassen und weiterzuentwickeln.

Google Maps: Internetdienst der Firma Google, der es ermöglicht, die geographische Lage von Orten oder Hotels auf einer Karte anzuzeigen.

GPL: Abk. für GNU General Public License

GUID: (Abk. für Globally Unique Identifier) weltweit eindeutige Identifikationsnummer für Hard- und Software, die bei der Verbindung ins Internet ausgelesen und an die jeweiligen Anbieter übertragen werden kann.

Hacienda: Deckname für ein Spionageprogramm des britischen Geheimdienstes GCHQ, mit dem die Behörde und Partnerdienste mittels Portscans ganze Länder auf IT-Schwachstellen scannen und kartieren.

Hash: Prüfsumme, mit der die Unversehrtheit einer erhaltenen E-Mail-Nachricht oder eines heruntergeladenen Antivirenprogramms überprüft werden kann.

Header: (dt. „Vorspann“) Metadaten, die am Anfang einer Datei stehen. So enthält die Kopfzeile einer E-Mail-Nachricht Informationen über Absender, Empfänger, Datum und Betreff der Nachricht.

Hierarchische Suche: die Recherche in Bibliothekskatalogen oder im Internet wird mit Stichwörtern ausgeweitet, die der ursprünglichen Suchanfrage unter- oder übergeordnet sind.

HTTP: (Abk. für Hypertext Transfer Protocol) Internetprotokoll zur Übertragung von Webseiten

HTTPS: (Abk. für Hypertext Transfer Protocol Secure) Internetprotokoll zur abhörsicheren Übertragung von Daten zwischen Web-Server und Browser

ID3 Tag: (Abk. für Identify an MP3) enthält Angaben zu Interpreten, Albumtitel, Erscheinungsjahr und Musikgenre, die direkt in der (MP3)Audiodatei abgespeichert sind.

IPbürgR: Internationaler Pakt über bürgerliche und politische Rechte

IMAP: (Abk. für Internet Message Access Protocol) Protokoll, über das Nutzer ihre E-Mails auf dem E-Mail-Server speichern und verwalten können. Die Nutzer mehrerer PCs müssen so ihre E-Mails nicht mehr wechselseitig abgleichen, sondern haben einen einheitlichen Zugriff auf die Informationen.

IMEI: (Abk. für International Mobile Station Equipment Identity) 15-stellige Gerätenummer des Handys, anhand der das Handy weltweit eindeutig identifiziert werden kann. Der Netzteilnehmer kann den IMEI-Code seines Handys mit der Eingabe *#006# abfragen.

Impressum: Anbieterkennzeichnung von Webseiten. Im Falle einer Online-Zeitung müssen Name und Anschrift des verantwortlichen Redakteurs, des Verlages oder des Herausgebers angeführt werden. Der Nutzer muss nämlich wissen, wohin er Leserbriefe senden kann, an wen er die Gegendarstellung richten muss und wer der Betreiber der Webseite ist, falls er rechtliche Ansprüche gegen diesen durchsetzen will.

IMSI: (Abk. für International Mobile Subscriber Identity) SIM-Kartennummer, die auf der SIM-Karte abgespeichert ist und beim Abschluss eines Handyvertrages eindeutig dem Mobilfunkteilnehmer zugeordnet wird. Mithilfe der SIM-Kartennummer kann der Mobilfunkteilnehmer weltweit eindeutig identifiziert werden.

Indexieren: Aufnahme eines Dokuments in den Datenbestand einer Suchmaschine sowie seine inhaltliche Erschließung

Informationskompetenz: Fähigkeit, den eigenen Informationsbedarf zu erkennen, ihn artikulieren zu können, Informationen effektiv zu suchen, die Informationen zu beurteilen und sinnvoll für die eigenen Belange einsetzen zu können.

Informationsarbeit: Suchen, Bewerten und Nutzen von Informationen

Integrität: Grundwert der IT-Sicherheit und bedeutet, dass die Daten nicht unbefugt verändert werden dürfen und dass jede Änderung nachvollziehbar sein muss.

IP-Adresse: (Abk. für Internet Protocol) einmalige Nummer, mit der PCs im Internet und in lokalen Netzwerken eindeutig identifiziert werden können. Eine IP-Adresse im IPv4-Format setzt sich aus vier Zahlenblöcken mit jeweils einer bis drei Ziffern (Zahlen 0 bis 255) zusammen, die durch Punkte getrennt sind, wie z. B. 217.199.0.35. Das IPv4-Format ermöglicht etwa 4,3 Milliarden verschiedene Adressen.

IPTC: (Abk. für International Press Telecommunications Council) Standard, der zur Speicherung von Metadaten zu Bildinhalten dient.

ISBN: (Abk. für International Standard Book Number) dient der weltweit eindeutigen Kennzeichnung von Büchern, Zeitschriften und anderen Publikationen.

Jailbreak: (dt. „Gefängnisausbruch“) Entfernen von Nutzungsbeschränkungen bei Apple-Geräten. Nach dem Jailbreack kann der Nutzer beliebige, von Apple nicht freigegebene Apps installieren.

JPEG: (Abk. für Joint Photographic Experts Group) Bildformat, das im Web für Bilder und Grafiken mit feineren Farbverläufen verwendet wird. Der Vorteil des JPEG-Formats ist die Komprimierung der Dateigröße ohne sichtbaren Qualitätsverlust der Bilder.

Kommentar: bei Facebook eine Anmerkung, die Nutzer zu Postings auf ihrer eigenen Pinnwand oder anderen Webseiten abgeben. Der Kommentar erscheint mit Profilbild des Autors unterhalb des ursprünglich geposteten Inhalts.

Kryptologe: Experte, der mathematische Verfahren und Techniken der Ver- und Entschlüsselung von Nachrichten entwickelt, analysiert und überprüft, etwa beim Homebanking oder verschlüsseltem E-Mail-Verkehr.

Kryptologie: Wissenschaft von der Ver- und Entschlüsselung von Daten und Telekommunikation.

Lauschangriff: geheime Überwachung eines Verdächtigen mithilfe einer versteckten Abhöranlage, um eine Straftat aufzuklären oder zu vereiteln.

L: legge, Gesetz

Leistungsschutzrecht: zum Urheberrecht verwandtes Schutzrecht. Es schützt nicht die Interessen der Kreativen, sondern die der Werkvermittler, wie Schauspieler, Verlage oder Tonträgerhersteller.

„Like“-Button: siehe „Gefällt-mir“-Button

Linkfarm: Gruppe von wechselseitig verlinkten Webseiten mit dem Ziel, die Ergebnisse von Suchmaschinen zu manipulieren. Die verlinkte Webseite soll für Suchanfragen auf die vorderen Plätze der Trefferliste gebracht werden, um dem Nutzer der Suchmaschine eine hohe Popularität der Webseite vorzutäuschen.

Listen: mithilfe von Listen kann man bei Facebook die eigenen Kontakte in Gruppen unterteilen. Über Listen kann man Informationen nur für bestimmte Gruppen sichtbar machen.

Lizenzvertrag: Vertrag, mit dem der Inhaber des Urheberrechts anderen Personen gegen eine Vergütung erlaubt, das Werk in einer bestimmten Art und Weise zu nutzen oder auch zu vermarkten.

Malware: Oberbegriff für Computerprogramme, welche unerwünschte Software-Aktivitäten ausführen und so die Sicherheit und Funktionsfähigkeit von Computern beeinträchtigen.

Markieren: bedeutet bei Facebook, dass man einen Link von einer Statusmeldung, einem Kommentar, einem Foto oder Video zum Facebook-Profil des markierten Freundes setzt.

Matthäus-Effekt: „Wer da hat, dem wird gegeben“, heißt es im Matthäusevangelium. Nach dem Matthäus-Effekt funktioniert beispielsweise auch die Suchmaschine Google. Populäre Webseiten werden noch populärer, weil sie in den Suchergebnissen vorne gelistet werden, deshalb von den Suchenden gefunden, angeklickt und wiederum neu verlinkt werden.

Metadaten: „Daten über Daten“. Solche Zusatzinformationen beinhalten viele Datenformate, wie .pdf, .jpeg, .cr2 oder .docx. Ein PDF-Dokument kann Verfasser, Erstellungsdatum, Änderungsdatum sowie Anwendungstool enthalten; ein Foto Kameratyp, Blende, Belichtung, ISO-Empfindlichkeit oder GPS-Koordinaten; ein Word-Dokument Verfasser, letzte Änderung oder die Bearbeitungshistorie.

MSISDN: (Abk. für Mobile Station Integrated Services Digital Network Number) weltweit eindeutige Rufnummer für Mobiltelefone. Die Rufnummer ist maximal 15-stellig und setzt sich zusammen aus der Landeskennzahl (Italien = 39), der Netzkennzahl des Dienstanbieters und der Teilnehmernummer.

Nachricht: innerhalb von Facebook eine private Information an einen Empfänger. Voraussetzung dafür ist, dass der Absender der Nachricht mit dem Empfänger derselben bei Facebook befreundet ist.

NFC: (Abk. für Near Field Communication) internationaler Standard zum kontaktlosen Datenaustausch. Die NFC-Technik wird auch zum mobilen Bezahlen eingesetzt. Der Nutzer hält hierbei im Laden quasi „im Vorbeigehen“ sein Smartphone oder seine Kreditkarte kurz vor das Lesegerät.

NSA: (Abk. für National Security Agency) US-amerikanischer Geheimdienst

OPAC: (Abk. für Online Public Access Catalogue) online verfügbarer Bibliothekskatalog, welcher der Literaturrecherche in den angeschlossenen Bibliotheken dient.

Open Access: Lizenzmodell für wissenschaftliche Publikationen im Internet, das erlaubt, diese frei und kostenlos zu nutzen.

OpenPGP: (Abk. für Open Pretty Good Privacy) ist ein internationaler Standard für Verschlüsselungssoftware, der dazu dient, E-Mails zu verschlüsseln sowie den Absender der Nachricht zweifelsfrei zu identifizieren. Der Anwender erstellt auf seinem PC selbst das OpenPGP-Schlüsselpaar und lässt den öffentlichen Schlüssel von seinen Freunden und Bekannten beglaubigen, eine zentrale Zertifizierungsstelle (Certification Authority, CA) fehlt. Auf den OpenPGP-Standard setzen beispielsweise die Projekte „Gpg4win“ (http://www.gpg4win.de) sowie „GnuPT“ (http://www.gnupt.de).

Open-Source-Software: Software, deren Quellcode für Dritte einsehbar ist. Open-Source-Lizenzen können darüber hinaus wie Freie Software erlauben, die Software beliebig zu nutzen, in eigene Programme zu integrieren, zu kopieren, zu verändern und wieder in den Umlauf zu bringen.

OpenStreetMap: eine freie Wiki-Weltkarte, die es ermöglicht, die geographische Lage von Orten, Straßen und Gebäuden auf einer Karte anzuzeigen. Die Daten stehen unter der CC-Lizenz, können also frei heruntergeladen und genutzt werden.

Opt-in-Prinzip: eine Regelung, bei der Newsletter nur erlaubt sind, wenn der Empfänger vorher informiert wurde und bewusst zustimmt, dass er mit der Zusendung der Newsletter einverstanden ist.

Opt-out-Prinzip: eine Regelung, bei der der Nutzer aktiv werden muss, um seine Privatsphäre zu schützen. So müssen die Nutzer bei Facebook die Voreinstellungen überarbeiten, um Informationen von „öffentlich“ auf „privat“ umzustellen. Schaltet der Nutzer etwa die Gesichtserkennung nicht ab, ist sie aktiv.

Paraphrase: sinngemäße oder auch verdeutlichende Wiedergabe von Textausschnitten mit eigenen Worten

PDF: (Abk. für Portable Document Format) von der Firma Adobe entwickeltes, plattformübergreifendes Dateiformat, das zum Erstellen elektronischer Dokumente dient.

Peer-Review: Begutachtung (review) wissenschaftlicher Arbeiten durch Wissenschaftlerkollegen (peers), wodurch die Qualität der wissenschaftlichen Publikationen sichergestellt werden soll.

Peer-to-Peer: (P2P) Datenaustausch von „Gleich zu Gleich“, ein zentraler Server fehlt. In einem Peer-to-Peer-Netz können Endgeräte gleichzeitig Dienste und Daten in Anspruch nehmen und anbieten.

Phrasen-Suche: Suche nach einer bestimmten Wortfolge in der Websuche. Enthält ein Dokument genau die gesuchte Wortfolge, wird diese im Suchergebnis angezeigt.

Pixel: Bildpunkt auf dem Monitor. Jeder Bildpunkt ist quadratisch und hat einen eindeutig definierten Farbwert. Die tatsächliche Abbildungsgröße eines Fotos auf dem Monitor hängt von der Anzahl der Pixel des Fotos und der Monitorauflösung ab. Hat das Foto 600 Pixel Breite mit 300 dpi Auflösung, erhält man eine Fotobreite von 2 Zoll, also 5 cm. Bei demselben Foto mit 60 dpi Auflösung erhält man ein Foto in einer Breite von 10 Zoll, also 25 cm.

Plagiat: Diebstahl „geistigen Eigentums“. Ein Plagiat liegt vor, wenn jemand fremde Texte oder Textteile, Gedankengänge oder Thesen in sein eigenes Werk übernimmt, ohne dies kenntlich zu machen. In der Wissenschaft stellt ein Plagiat - je nach Schwere und Umfang - einen Verstoß gegen die Regeln „guter wissenschaftlicher Praxis“ dar.

Podcast: Audiodatei, die sowohl Sprache als auch Musik zum Inhalt haben kann. Podcasts können aus dem Internet mithilfe spezieller Software (Podcatcher) abonniert und heruntergeladen und zu jedem beliebigen Zeitpunkt auf einem MP3-Player abgespielt werden.

Podcatcher: Software zum Abonnieren von Podcasts

POP: (Abk. für Post Office Protocol) ein Internetprotokoll für das Herunterladen von E-Mails von einem E-Mail-Server auf den PC

Posten: Inhalte wie Texte, Kommentare, Fotos oder Links auf einer Facebook-Pinnwand veröffentlichen.

PPI: (Abk. für Pixel per Inch) Einheit, die angibt, wie viele Pixel pro Zoll (= 2,54 cm) vorhanden sind. Je mehr Pixel pro Zoll existieren, desto feinere Farbverläufe eines Bildes sind möglich.

Prepaidkarten: (dt. vorausbezahlt) Kartenhandys, die bereits beim Kauf vorab in bar bezahlt werden.

Presseschau: redaktionelle Zusammenfassung von tagesaktuellen Meldungen zu einem Thema aus Printmedien, Internet, Fernsehen oder Radio.

Primärliteratur: Werk eines Autors, Forschungsergebnis eines Wissenschaftlers oder Quellenwerk wie ein Gesetz oder eine Urkunde (vgl. Sekundärliteratur).

Prism: Deckname für ein Spionageprogramm des US-Geheimdienstes NSA, mit dem die Behörde auf Nutzerdaten großer amerikanischer IT-Firmen wie Facebook, Google, Microsoft, Apple, YouTube oder Yahoo zugreifen, sie analysieren und auswerten kann.

Privacy by Default: Konzept des Datenschutzes, bei dem per Voreinstellung in Software, Apps oder Webdienste der Schutz der Privatsphäre vorgesehen ist. Für Facebook würde das beispielsweise bedeuten, dass Profildaten standardmäßig nicht öffentlich wären und dass der Nutzer aktiv werden müsste, möchte er diese für alle Facebooker sichtbar machen. Ohne Wissen und gegen den Willen der Nutzer werden keine Personendaten gesammelt.

Privacy by Design: Konzept des Datenschutzes, bei dem datenschutzfreundliche Prinzipien wie Datenvermeidung, Datensparsamkeit oder Zweckbindung bereits in die Technik eingebaut sind. Das bedeutet zum Beispiel für einen Cloud-Dienst, dass dieser zum Schutz der Vertraulichkeit der abgelegten Daten eine Ende-zu-Ende-Verschlüsselung anbietet.

Proprietäre Software: herkömmlich lizenzierte kommerzielle Software. Der Quellcode ist nicht frei zugänglich, sodass er weder angepasst noch weiterentwickelt werden kann. In der Regel unterliegt sie dem klassischen Urheberrecht.

Provider: in der Regel versteht man damit den Zugangsvermittler zum Internet.

Providervertrag: Vertrag, der den Zugang zum Internet regelt.

Proxy: (dt. Vermittler in einem Netzwerk) nimmt Anfragen des Nutzers entgegen und leitet sie über die eigene IP-Adresse an den Webserver weiter. Der Nutzer erhält die angefragte Webseite nicht vom Webserver, sondern vom gewählten Proxy.

Public-Key-Verfahren: Verschlüsselungsverfahren, das mit einem privaten und einem öffentlichen Schlüssel arbeitet. Authentizität und Integrität der E-Mail-Nachricht werden sichergestellt, indem der Absender diese mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und der Empfänger sie mit seinem privaten Schlüssel entschlüsselt.

PUK: (Abk. für Personal Unblocking Key) achtstelliger Code, der zum Entsperren der SIM-Karte nach 3-maliger Falscheingabe der PIN dient. Die PUK-Nummer ist dem Betreiber des Telefondienstes bekannt.

Push-Nachricht: eine Kurznachricht, welche direkt auf dem Display des Empfängers angezeigt wird, ohne dass die entsprechende App geöffnet sein muss.

RAW: (dt. roh, unbearbeitet) Fotoformat, dessen Vorteil darin besteht, dass der Nutzer im Nachhinein am PC die geschossenen Fotos nachbearbeiten kann, wie die Belichtung, den Kontrast oder die Farbsättigung. Das Raw-Format wird bei Spiegelreflexkameras verwendet.

Regin: Spionageprogramm des amerikanischen und britischen Geheimdienstes, das für Angriffe auf EU-Behörden, Unternehmen, Telefonanbieter, Forschungsinstitute und Einzelpersonen eingesetzt wird. Offenbar kann das Programm auf infizierten Rechnern Screenshots machen, Passwörter auslesen, den Datenverkehr überwachen, gelöschte Dateien wieder herstellen und Anrufe abfangen.

QR-Code: (dt. „schnelle Antwort“) Quadrat, in dem Informationen durch schwarze und weiße Punkte dargestellt werden. Ein QR-Code kann u. a. Informationen zu Webadressen, Telefonnummern, Sehenswürdigkeiten oder Produkten enthalten, die von Smartphones oder Tablets eingescannt und ausgelesen werden können.

Quantified Self: (dt. Selbstvermessung) Sammeln von Daten über den eigenen Körper und das eigene Leben, um die Daten zu analysieren, auszuwerten und zu diskutieren.

Quellcode: Programmcode, der vom Programmierer erstellt wird. Der Quellcode muss in die sogenannte Maschinensprache übersetzt werden, dass er vom Computer verstanden wird. Der Anwender sieht nur die Programmoberfläche, über die er Befehle und Abfragen eingibt. Bei Open Source-Projekten ist der Quellcode offen, sodass er von anderen studiert, weiterentwickelt oder an eigene Bedürfnisse angepasst werden kann.

Redaktion: Gesamtheit der Redakteure einer Zeitung, eines Rundfunks oder Fernsehens. Die Redakteure berichtigen, ergänzen oder kürzen Beiträge, legen Überschriften fest und wählen die passenden Fotos oder Multimediaelemente zur Veröffentlichung aus.

Referrer: (dt. Verweis) Internetadresse der Webseite, von der der User durch einen Klick auf einen Link auf die Anbieterseite gelangt.

Roaming: (dt. Durchleitung) der Handynutzer kann über einen anderen Mobilfunkbetreiber Anrufe empfangen und tätigen. Über Roaming sind Handynutzer auch im Ausland unter ihrer Rufnummer erreichbar. Voraussetzung für Roaming ist, dass das Handy den Mobilfunkstandard des Gastnetzes unterstützt und dass zur Kostenabrechnung ein Roaming-Abkommen zwischen dem Betreiber beider Mobilfunknetze besteht.

Root: (dt. Wurzel) verschafft dem Handynutzer die größtmöglichen Rechte (Administratorenrechte) über sein Android-Handy. Befreit von den ursprünglichen Rechte-Fesseln des Herstellers kann der Nutzer etwa eine Firmware auf das Handy aufspielen.

RSS: (Abk. für Really Simple Syndication) Technik, mit der sich Artikel einer Webseite, Aktualisierungen eines Blogs oder Bookmark-Sammlungen als Feed abonnieren lassen.

RSS-Reader: Programm, das RSS-Feeds sammelt und anzeigt.

Schlagwort: Begriff, der den Inhalt einer Publikation beschreibt. Schlagwörter werden auf der Grundlage eines normierten Begriffsverzeichnisses von Fachleuten vergeben.

Sekundärliteratur: Literatur, die sich mit dem Werk eines Autors oder mit der Theorie und den Forschungsergebnissen eines Wissenschaftlers auseinandersetzt (vgl. Primärliteratur).

SEO: (Abk. für Search Engine Optimization) alle Maßnahmen, die dazu führen, dass Webseiten in den Suchergebnissen der Suchmaschinen auf den ersten Plätzen erscheinen.

Shitstorm: Welle der Empörung und Kritik in sozialen Medien, Blogs oder Foren, die zum Teil unsachlich und beleidigend geführt wird.

S.I.A.E.: (Abk. für Società Italiana degli Autori ed Editori) italienische Verwertungsgesellschaft für Autoren und Verleger. Wer fremde Werke nutzen möchte, schließt in der Regel nicht mit den einzelnen Autoren und Verlagen Lizenzverträge ab, sondern mit der S.I.A.E.

Signatur: Folge von Buchstaben und Zahlen, die dazu dienen, Literatur in Bibliotheken zu identifizieren und auffindbar zu machen.

Sitemap: Liste aller Webseiten, die zu einer Homepage gehören. In der Regel zeigt die Sitemap auch die hierarchische Gliederung samt Links auf. Die User erhalten über Sitemap einen Überblick über Struktur und Umfang des Internetauftritts.

Skalierung: in der digitalen Bildbearbeitung wird die Größe eines Bildes, also die Anzahl der Pixel, verändert.

S/MIME: (Abk. für Secure Multipurpose Internet Mail Extensions) Verschlüsselungstechnik, die auf dem Public-Key-Verfahren aufbaut und mit deren Hilfe Nutzer Dateien lokal ver- und entschlüsseln können. Die Authentizität des öffentlichen Schlüssels wird durch X.509-Zertifikate von akkreditierten Zertifizierungsstellen sichergestellt.

SSID: (Abk. für Service Set Identifier) Name des WLAN-Netzwerkes. Der Betreiber des WLAN-Routers kann den Namen des WLAN-Funknetzes frei wählen. In der Regel kann der Betreiber das eigene WLAN auch unsichtbar machen. Einen wirklichen Schutz bietet dies nicht, weil Profis auch unsichtbare WLAN-Netze sichtbar machen können.

SSL: (Abk. für Secure Sockets Layer) Protokoll, das dafür sorgt, dass zwischen Browser und Webserver ein „sicherer Kanal“ aufgebaut wird, sodass Unberechtigte den Datenverkehr nicht belauschen können. Der Nutzer erkennt eine SSL-Verbindung an der Protokollangabe „https://“ in der Adresszeile und am geschlossenen Vorhängeschloss.

Stichwort: Wort, das der inhaltlichen Erschließung eines Dokuments dient und als solches im Dokument vorkommen muss. Es können auch sämtliche Wörter eines Dokuments als Stichworte in einem Index (Stichwortverzeichnis) aufgenommen werden.

Statusleiste: Funktion bei Facebook, die sich auf der Facebook-Chronik befindet. Nutzer können darüber neben dem Status, Fotos und dem Ort auch ihre Lebensereignisse posten.

Status-Update: in Facebook eine Nachricht, die der Benutzer an seine Facebook-Freunde sendet.

Streaming: gleichzeitiges Herunterladen und Abspielen von Audio- und Videodateien. Man spricht auch vom Webradio und Web-TV.

Suchbegriff: Wort, mit dem in einer Suchmaschine oder einem Bibliothekskatalog gesucht wird.

Suchmaschine: Programm, das im Internet oder in einem PC (Desktopsuchmaschine) nach Dokumenten recherchiert. Nach der Eingabe des Suchbegriffs liefert die Suchmaschine eine Trefferliste auf möglicherweise für den Nutzer relevante Dokumente. Die bekannteste Suchmaschine ist Google (https://www.google.com/), eine datenschutzfreundliche ist startpage (https://startpage.com/).

Suchmaske: Eingabefeld einer Suchmaschine oder eines Webkatalogs, in das Suchbegriffe eingegeben werden können.

Tag: Schlagwort, das Texte, Bilder, Videos oder Audios beschreibt. Die Tags können frei gewählt werden, einen Schlagwortkatalog wie bei Bibliotheken gibt es bei Web 2.0-Diensten nicht.

Tauschbörse: (Filesharing- oder Peer-to-Peer-System) beruht auf dem Grundsatz „Geben und Nehmen“ und ermöglicht dem Nutzer, Dateien (Texte, Fotos, Videos) vom eigenen PC zum Download anzubieten und selbst Dateien von anderen Nutzern herunterzuladen, also zu kopieren.

TCP/IP: (Abk. für Transmission Control Protocol/Internet Protocol) Internet-Protokoll, das für den Datenaustausch zwischen vernetzten PCs sorgt. Die IP-Adresse ist sozusagen die „Postanschrift“, an die ein Datenpaket gesendet wird.

Tempora: Deckname für ein Spionageprogramm des britischen Geheimdienstes GCHQ, mit dem E-Mails, Chats oder Telefonate zwischengespeichert werden. Dazu zapft GCHQ heimlich Glasfaser- und Seekabel an, über die der internationale Datenverkehr läuft. Die Inhalte werden drei Tage (full take), die Metadaten 30 Tage gespeichert.

Tor: Freeware-Tool zum anonymen Surfen im Netz (https://www.torproject.org/)

TrustCenter: (Certificate Authority, CA) prüft die Identität einer bestimmten Person und beglaubigt die Zugehörigkeit eines öffentlichen Schlüssels zu dieser Person, indem sie das digitale Zertifikat (X.509-Zertifikat) mit ihrem privaten Schlüssel signiert.

Trunkierung: (dt. abschneiden) ein Suchbegriff wird teilweise durch Platzhalter (*, ?, %) ersetzt, sodass bei einer Recherche stets verschiedene Wortfolgen einbezogen werden können.

Tweet: (dt. zwitschern) bezeichnet eine kurze, maximal 140 Zeichen lange Nachricht innerhalb des sozialen Netzwerkes Twitter.

Urheberrecht: schützt den Urheber geistiger Werke, wie Texte, Fotos, Filme oder Software. Der Urheber hat das ausschließliche Recht zu entscheiden, ob und in welcher Weise er sein Werk wirtschaftlich verwerten will.

Verlag: Unternehmen, das schöpferische Werke wie Manuskripte erwirbt, diese lektoriert, für den Druck oder für E-Books vorbereitet, die Druck-Erzeugnisse herstellt, Marketing betreibt und verkauft.

Verfügbarkeit: Grundwert der IT-Sicherheit und bezweckt, dass Daten trotz plötzlichen Datenverlustes abrufbar sind. Die Verfügbarkeit der Daten kann durch ein regelmäßiges Backup auf verschiedenen Datenträgern gesichert werden.

Verordnung: Rechtsnorm, die vom Ministerrat erlassen und vom Präsidenten der Republik in Form eines Dekretes verlautbart wird.

Verschlüsselung: Verfahren, welches eine lesbare in eine unlesbare Information umwandelt. Ziel der Verschlüsselung ist, die Vertraulichkeit - etwa einer E-Mail-Nachricht - sicherzustellen.

Vertraulichkeit: Grundwert der IT-Sicherheit und bedeutet, dass nur berechtigte Personen Zugriff auf vertrauliche Daten haben.

Völkerrecht: Rechtsordnung, welche insbesondere die Beziehung zwischen Staaten regelt. Völkerrecht entsteht in erster Linie durch Verträge, die sich mit Fragen des Weltfriedens und der internationalen Sicherheit, des internationalen Handels und dem Schutz der Menschenrechte beschäftigen.

Vorratsdatenspeicherung: Verbindungsdaten, die Mobilfunkanbieter und Provider für einen bestimmten Zeitraum für die Behörden speichern und vorrätig halten müssen. Dazu zählt etwa wer mit wem, wie lange, wann und wo telefoniert, wer wem eine E-Mail gesendet oder wer welche Webseiten aufgerufen oder wer welche Medieninhalte auf Webseiten hochgeladen hat. Um die Personen identifizieren zu können, die hinter den IP-Adressen und Rufnummern stehen, müssen die Verbindungsdaten mit den Bestandsdaten verknüpft werden.

Web 2.0: damit wird der Wandel des Internets vom Informationsmedium zum Mitmachnetz gekennzeichnet. Die Nutzer lesen nicht nur, sondern erstellen selbst Inhalte, indem sie Produktbewertungen abgeben, Musik und Filme kommentieren und indem sie ihre Fotos und Videoclips auf Portale hochladen, um sie der Öffentlichkeit vorzustellen.

Webkatalog: thematisches Verzeichnis im Internet, das URLs von Webseiten zu einzelnen Themen in einem „Katalog“ zusammenfasst, z. B. eine Auswahl von Webseiten zum Thema Computer. DMOZ – Open Directory Project (http://www.dmoz.org/) ist ein kostenloser und freier Webkatalog.

Webformular: wird auf Webseiten zum Erfassen von Daten eingesetzt. Es wird beispielsweise in Web-Mail-Anwendungen oder beim Anmelden in einem Online-Shop verwendet.

Webserver: Computer, auf dem Webseiten und Medieninhalte abgelegt sind sowie Internetdienste angeboten werden, die vom Nutzer in der Regel per Browser angefordert werden können.

Whistleblower: (dt. Enthüller) Mitarbeiter in Unternehmen oder in der öffentlichen Verwaltung, die Missstände wie Korruption oder Steuerhinterziehung aufdecken, indem sie diese beispielsweise an die Presse weitergeben. Der Whistleblower steht im Konflikt zwischen Loyalitätspflicht zum Arbeitgeber und öffentlichem Informationsinteresse.

Whois-Abfrage: Abfrage an die Registration Authority (RA, Registrierungsstelle), wer Inhaber einer Internetadresse ist.[256]

Widget: Miniprogramm auf dem Startbildschirm oder im Hauptmenü, wie Uhranzeige, Taschenrechner oder Terminkalender

WikiLeaks: Enthüllungsplattform im Internet, auf der Dokumente und Videos anonym veröffentlich wurden, die unter staatlicher und betrieblicher Geheimhaltung standen.

WLAN: (Abk. für Wireless Local Area Network) drahtloses lokales Netzwerk. Als Synonym für WLAN wird auch Wi-Fi genutzt.

WPA2: (Abk. für Wi-Fi Protected Access 2) Verschlüsselungstechnik für WLAN, die zurzeit höchsten Sicherheitsstandards genügt.

XMP: (Abk. für Extensible Metadata Platform) Standard, der zur Speicherung von Metadaten zu digitalen Medien dient.

X.509-Zertifikat: ein Standardformat für digitale Zertifikate, die sicherstellen, dass der öffentliche Schlüssel tatsächlich der angegebenen Person gehört (Public-Key-Verfahren). Ein X.509-Zertifikat beinhaltet in der Regel den Namen des Ausstellers (Certification Authority, CA), den Namen des Inhabers, die Gültigkeitsdauer sowie den Fingerprint.

XKeyscore: eine Art „Geheimdienst-Google“, mit dem der US-Geheimdienst NSA die Internetkommunikation nach beliebigen Suchkriterien filtern kann; etwa von welcher IP-Adresse aus bestimmte Google-Suchanfragen gestellt, bestimmte Webseiten aufgerufen, verschlüsselte E-Mails versendet wurden oder nach allen IP-Adressen, die in einer bestimmten Region eine bestimmte Browsersprache verwenden.

Zombie: ferngesteuertes Smartphone in einem Botnetz

256 NIC.it: http://www.nic.it/web-whois/index.jsf; DomainTools: http://www.domaintools.com

Literatur

Agamben, Giorgio (2004): *Ausnahmezustand*, Frankfurt a. M.

- (2014): *Die Geburt des Sicherheitsstaats,* Le Monde diplomatique Nr. 10360, 14.3.2014, http://www.monde-diplomatique.de/pm/2014/03/14.mondeText.artikel,a0065.idx,12

Amann, Susanne u. a. (2012): *Aus! Zeit!,* in: Der Spiegel 27/2012, S. 73-74.

Appelbaum, Jacob u. a. (2013): *Der geheime Werkzeugkasten der NSA,* Spiegel online, 30.12.2013 – 11:00 Uhr, http://www.spiegel.de/netzwelt/netzpolitik/neue-dokumente-der-geheime-werkzeugkasten-der-nsa-a-941153.html

- u. a. (2013): *Wie der US-Geheimdienst weltweit Rechner knackt,* Spiegel online, 30.12.2013 – 11:02 Uhr, http://www.spiegel.de/netzwelt/netzpolitik/quantumtheory-wie-die-nsa-weltweit-rechner-hackt-a-941149.html

- u. a. (2014): *NSA/GCHQ: Das HACIENDA-Programm zur Kolonisierung des Internet,* heise online 15.08.2014, http://www.heise.de/ct/artikel/NSA-GCHQ-Das-HACIENDA-Programm-zur-Kolonisierung-des-Internet-2292574.html

- u. a. (2014): *Das Five-Eyes-Botnetz. Die Besetzung des Internet durch die westlichen Geheimdienste,* in: c't 2014, Heft 22, S. 166-168.

- u. a. (2014): *Was die NSA knacken kann - und was nicht,* Spiegel online, 29.12.2014 – 10:06 Uhr, http://www.spiegel.de/spiegel/snowden-dokument-so-unterminiert-die-nsa-die-sicherheit-des-internets-a-1010534.html

- u. a. (2015): *Die NSA rüstet zum Cyber-Feldzug,* Spiegel online, 18.01.2015 – 14:00 Uhr, http://www.spiegel.de/netzwelt/netzpolitik/snowden-dokumente-wie-die-nsa-digitale-kriege-vorbereitet-a-1013521.html

Babiack, Ulrich (^{4}2001): *Effektive Suche im Internet*, Beijing u. a.

Bager, Jo u. a. (2013): *Digitale Identität schützen,* in: c't Security 2013, S. 146-149.

Bamford, James (2013): Interview, Journalist, der sich seit mehr als dreißig Jahren mit dem US-Geheimdienst NSA beschäftigt, Zeit online, 20.06.2013 - 08:00 Uhr, http://www.zeit.de/2013/26/nsa-geheimdienst-james-bamford

Barry, Max (2012): *Maschinenmann,* München.

Beckedahl, Markus u. a. (Hrsg.) (2013): *Überwachtes Netz. Edward Snowden und der größte Überwachungsskandal der Geschichte,* Berlin.

Becker, Konrad u. a. (Hrsg.) (2010): *Deep Search. Politik des Suchens jenseits von Google*, Bonn. Online unter: http://www.bpb.de/gesellschaft/medien/politik-des-suchens/

Bendrath, Ralf (2014): *Überwachungstechnologien,* in: APuZ 18-19/2014, http://www.bpb.de/apuz/183090/ueberwachungstechnologien

Berger, Daniel (2014): *Schützen und teilen. Social-Media-Buttons datenschutzkonform nutzen,* in: c't 2014, Heft 26, S. 148-151.

- (2014): *Selbstkontrolle. Wie Sie Ihre Facebook-Daten schützen,* in: c't 2015, Heft 1, S. 160-163.

Beuth, Patrick (2013): *Tor – die Tarnkappe fürs Netz,* Zeit online, 25.01.2013 - 10:15 Uhr, http://www.zeit.de/digital/datenschutz/2013-01/serie-mein-digitaler-schutzschild-tor-browser-bundle

- (2013): *Alles Wichtige zum NSA-Skandal,* Zeit online, aktualisiert 6.07.2014 - 12:16 Uhr, http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal

Bevc, Tobias (2011): *Überlegungen zum demokratischen Potential des Web 2.0,* Telepolis 27.08.2011, http://www.heise.de/tp/artikel/35/35283/1.html

Bieri, Peter ([4]2005): *Das Handwerk der Freiheit. Über die Entdeckung des eigenen Willens*, München Wien.

- (2013): *Eine Art zu leben. Über die Vielfalt menschlicher Würde,* München.

Biermann, Kai u. a. (2013): *US-Regierung zapft Facebook und Google an,* Zeit online, 07.06.2013 - 11:25 Uhr, http://www.zeit.de/digital/datenschutz/2013-06/USA-Geheimdienste-Daten-Internet-Verizon

- (2013): *Millionen SIM-Karten sind nicht sicher,* Zeit online, 21.07.2013 - 09:20 Uhr, http://www.zeit.de/digital/mobil/2013-07/sim-karte-hack-nohl

Binney, William (2013): Interview, ehemaliger NSA-Techniker und Whistleblower, Zeit online, 18.09.2013 - 14:05 Uhr, http://www.zeit.de/digital/datenschutz/2013-09/nsa-william-binney

Bleich, Holger (2013): *Mythos Anonymität. Von der Schwierigkeit, sich unerkannt im Internet zu bewegen,* in: c't 2013 Heft 20, S. 96-101.

Boehme-Neßler, Volker (2013): *Facebook-Demokratie,* heise online 03.03.2013, http://www.heise.de/tp/artikel/38/38611/1.html

Braun, Herbert (2014): *Undercover. Wie Google-Werkzeuge auf fremden Websites Daten sammeln,* in: c't 2014 Heft 11, S. 134-135.

Broca, Sébastien (2014): *Wie frei ist die Freie Software?* Le Monde diplomatique Nr. 10511, 12.9.2014, http://www.monde-diplomatique.de/pm/2014/09/12.mondeText.artikel,a0032.idx,5

Buchter, Heike (2013): *Die Profiteure,* Zeit online, 09.08.2013 - 18:22 Uhr, http://www.zeit.de/2013/33/nsa-spionage-industrie-profiteure

Bundesamt für Sicherheit in der Informationstechnik (BSI): *Wie bewege ich mich sicher im mobilen Netz?*, https://www.bsi-fuer-buerger.de/BSIFB/DE/MobileSicherheit/mobileSicherheit_node.html

Burke, Peter (2014): *Die Explosion des Wissens. Von der Encyclopédie bis Wikipedia*, Berlin.

Crueger, Jens (2013): *Privatheit und Öffentlichkeit im digitalen Raum: Konflikt und die Reichweite sozialer Normen,* in: APuZ 15-16/2013, http://www.bpb.de/apuz/157544/privatheit-und-oeffentlichkeit-im-digitalen-raum-konflikt-um-die-reichweite-sozialer-normen

Dambeck, Holger (2013): *Zeig mir deine Likes - und ich weiß, wer du bist,* Spiegel online, 11.03.2013 - 21:06 Uhr, URL: http://www.spiegel.de/netzwelt/web/facebook-studie-likes-enthuellen-persoenlichkeit-a-888151.html

Dworschak, Manfred u. a. (2012): *Planet der Freundschaft,* in: Der Spiegel 19/2012, S. 125-134.

Eckert, Svea u. a. Anika (2012): *Facebook - Milliardengeschäft Freundschaft,* NDR Mediathek, 45 Min, 02.04.2012 - 22:00 Uhr, http://www.ndr.de/fernsehen/sendungen/45_min/videos/minuten531.html

Eimer, Annick (2008): *„Jede zweite Meldung ist falsch“*, Zeit online 09.07.2008 - 12:35 Uhr, http://www.zeit.de/zeit-wissen/2008/04/interview-michael-haller

Endres, Johannes (2013): *Tracking-Schutz im Browser,* in: c’t Security 2013, S. 124-125.

Feibel, Thomas (2011): *Kinder, Internet & Pannen. Medienerziehung mit Verständnis und Augenmaß,* in: c’t 2011, Heft 21, S. 126-133.

Feldbauer-Durstmüller, Birgit (2007): *Richtlinien zum Verfassen wissenschaftlicher Arbeiten,* Johannes Kepler Universität Linz. Netzwerk für Forschung, Lehre und Praxis, http://http://www.uzr.at/uploads/media/Richtlinien_wiss-Arbeit_250907.pdf

Ferretti, Alessandro (2008): *Diritto d’autore. La tutela delle opere dell’ingegno nel diritto interno ed internazionale*, Napoli.

Fischermann, Thomas u. a. (2013) *Wer hebt das Datengold?* Zeit online, 03.01.2013 - 07:00 Uhr, http://www.zeit.de/2013/02/Big-Data

fluter. 2013/Nr. 46: *Ich bin dann mal web. Thema Internet,* http://www.fluter.de/de/120/heft/11422/

Franke, Fabian u. a. (2010): *Schlüsselkompetenzen: Literatur recherchieren in Bibliotheken und Internet*, Stuttgart, Weimar.

Friedrich, Anna (2008): *Google News verursacht Kurssturz bei United Airlines,* Themenblog, 19.09.2008, http://themenblog.de/2008/09/19/google-news-verursacht-kurssturz-bei-united-airlines/

Friedrich, Jörg (2012): *Kritik der vernetzten Vernunft. Philosophie für Netzbewohner,* Hannover.

Galison, Peter (2014): *Wir werden uns nicht mehr wiedererkennen,* FAZ, 07.04.2014 -17:16 Uhr, http://www.faz.net/aktuell/feuilleton/selbstzensur-durch-massenueberwachung-wir-werden-uns-nicht-mehr-wiedererkennen-12884520.html

Gantert, Klaus u. a. (^{8}2008): *Bibliothekarisches Grundwissen*, München.

Garante Privacy (2013): *Il Garante scrive a WhatsApp: come utilizzate i dati degli utenti italiani?* 27.02.2013, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2288310

Gauger, Jörg-Dieter u. a. (Hrsg.) (2010): *Bildung und Unterricht in Zeiten von Google und Wikipedia,* http://www.kas.de/wf/de/33.21634/; http://www.kas.de/wf/doc/kas_21634-544-1-30.pdf?110118165914

Gaycken, Sandro (2011): *Cyberwar. Das Internet als Kriegsschauplatz,* München.

Geiselberger, Heinrich (Hrsg.) (2011): *WikiLeaks und die Folgen,* Berlin.

Gibney, Alex (2010): *Taxi zur Hölle*, ARD, 21.10.2010, 20:15 Uhr.

Greveler, Ulrich u. a (2012): *Identifikation von Videoinhalten über granulare Stromverbrauchsdaten,* Labor für IT-Sicherheit Fachhochschule Münster, http://1lab.de/pub/GrJuLo_Smartmeter.pdf

Häntzschel, Jörg (2014): *Jeder könnte ein Terrorverdächtiger sein,* Sueddeutsche.de, 24.07.2014 - 20:07 Uhr, http://www.sueddeutsche.de/politik/irrwitziges-handbuch-der-us-geheimdienste-jeder-koennte-ein-terrorverdaechtiger-sein-1.2061380

Hartmann, Martin (2011): *Die Praxis des Vertrauens*, Berlin.

Heller, Christian (2011): *POST-PRIVACY. Prima leben ohne Privatsphäre,* München.

Holland, Martin (2013): *Alles unter Kontrolle. IT-Techniker lässt US-Lauschsystem aufliegen,* in: c't 2013, Heft 14, S. 16-17.

Hotter, Maximilian (2011): *„Privatsphäre". Der Wandel eines liberalen Rechts im Zeitalter des Internets,* Frankfurt a. M.

Hughes, Eric (2013): Interview, Mathematiker und Cypherpunk-Gründer, Zeit online, 20.09.2013 - 16:56 Uhr, http://www.zeit.de/digital/internet/2013-09/cypherpunks-eric-hughes

Jansson, Kurt u. a. (2006): *Wikipedia: Kreative Anarchie für den freien Informations- und Wissensaustausch*, in: Drossou, Olga u. a. (Hrsg.) (2006): *Die wunderbare Wissensvermehrung. Wie Open Innovation unsere Welt revolutioniert*, Hannover.

Kirk, Michael u. a. (2014): *Die geheimen Staaten von Amerika. 1. Angriff auf die Privatsphäre,* ZDFinfo, 27.05.2014, 21:00 Uhr

- (2014): *Die geheimen Staaten von Amerika. 2. NSA - Operation Allmacht,* ZDFinfo, 27.05.2014, 21:40 Uhr

- (2014): *Die geheimen Staaten von Amerika. 3. Jagd auf die Whistleblower,* ZDFinfo, 28.05.2014, 10:15 Uhr

Kleinz, Torsten (2013): *Wie abhörsicher ist Skype wirklich?* Zeit online, 31.07.2012 - 17:42 Uhr, http://www.zeit.de/digital/datenschutz/2012-07/skype-ueberwachung

Koch, Werner u. a. (2010): *Das Gpg4win-Kompendium. Sichere E-Mail- und Datei-Verschlüsselung mit GnuPG für Windows.* Version 3.0.0, 21.05.2010, http://www.gpg4win.de/doc/de/gpg4win-compendium.html

Kossel, Axel u. a. (2013): *Raus aus der Cloud-Falle,* in: c't 2013, Heft 11, S. 113-114.

- u. a. (2013): *Tarnkappen. Verschlüsselung und Anonymität erschweren das Datenschnüffeln,* in: c't 2013, Heft 16, S. 118-119.

Krol, Ariane u. a. (2013): *Spione des Marktes. Was Werbung im Internet alles kann,* Le Monde diplomatique Nr. 10130, 14.6.2013, http://www.monde-diplomatique.de/pm/2013/06/14.mondeText.artikel,a0056.idx,22

Kuhlen, Rainer (1999): *Die Konsequenzen von Informationsassistenten. Was bedeutet informationelle Autonomie oder wie kann Vertrauen in elektronische Dienste in offenen Informationsmärkten gesichert werden?* Frankfurt a. M.

Kurz, Constanze u. a. (2011): *Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen,* Frankfurt a. M.

Kurzedim, Michael (2004): *Wissenswettstreit. Die kostenlose Wikipedia tritt gegen die Marktführer Encarta und Brockhaus an*, in: c't 2004, Heft 21, S. 132-139.

Lang, Mirco (2014): *Nehmen und geben. Open-Source-Lizenzen und ihre Implikationen,* in: c't 2014, Heft 15, S. 144-149.

Lanier, Jaron (2014): *Wem gehört die Zukunft? Du bist nicht der Kunde der Internet-Konzerne, du bist ihr Produkt,* Hamburg

- (2014): *Für einen neuen Humanismus. Wie wir der digitalen Entrechtung entkommen,* in: „Blätter" 11/2014, S. 43-58.

Lessig, Lawrence (2010), Interview, Gründer der Creative-Commons-Initiative, Seuddeutsche.de, 17.05.2010 - 21:26 Uhr, http://www.sueddeutsche.de/kultur/lawrence-lessig-im-interview-es-geht-nicht-darum-madonnas-musik-zu-stehlen-1.439603

- (2012), *Der Vietnam-Krieg des Internets,* Handelsblatt, 01.02.2012 - 10:02 Uhr, http://www.handelsblatt.com/meinung/gastbeitraege/gastbeitrag-der-vietnam-krieg-des-internets/6136040.html

Lischka, Konrad (2010): *Wie Handys die Welt beobachten,* Spiegel online, 23.06.2010 – 19:42 Uhr, http://www.spiegel.de/netzwelt/web/verhaltensueberwachung-wie-handys-die-welt-beobachten-a-701230.html

- (2013): *Das Märchen vom anonymen Bewegungsprofil,* Spiegel online, 31.03.2013 – 19:13 Uhr, http://www.spiegel.de/netzwelt/web/mobilfunkspuren-lassen-sich-leicht-menschen-zuordnen-a-891850.html

Lohmann, Michael (2006): *„Wer nichts zu verbergen hat, hat auch nichts zu befürchten"*, Telepolis 27.09.2006, http://www.heise.de/tp/artikel/23/23625/1.html

Luhmann, Niklas (1989): *Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität*, Stuttgart.

Machill, Marcel (^{2}2009): *12 goldene Suchmaschinen-Regeln. Ein Ratgeber für Verbraucherinnen und Verbraucher, die sich besser und sicherer im Internet zurecht finden wollen,* Landesanstalt für Medien Nordrhein-Westfalen (Hrsg.), http://www.lfm-nrw.de/fileadmin/lfm-nrw/Medienkompetenz/ratgeber-suchmaschinen-farbe.pdf

Martienssen, Daniel (2013): *Die Rückkehr des Leviathan,* derFreitag, 05.07.2013 - 09:10 Uhr, http://www.freitag.de/autoren/danielm2601/die-rueckkehr-des-leviathan

McLaughlin, Catriona (2013): *Die Besserwisser,* Zeit online, 05.07.2013 - 18:38 Uhr, http://www.zeit.de/2013/28/acxiom

Meister, Dorothee M. u. a.(2008): *Medienkompetenz als lebenslange Herausforderung,* in: UNESCO heute 1/2008: *Wissen im Web,* S. 53-55; online: http://www.unesco.de/fileadmin/medien/Dokumente/unesco-heute/uh1-2008/uh108_s53-55.pdf

Miller, Daniel (2012): *Das wilde Netzwerk. Ein ethnologischer Blick auf Facebook*, Berlin.

Moglen, Eben (2014): *Die Privatsphäre wurde halb verkauft, den Rest hat die Regierung gestohlen,* irights.info, 05.06.2014, http://irights.info/artikel/die-privatsphaere-wurde-halb-verkauft-den-rest-hat-die-regierung-gestohlen/23369

Möller, Erik (2005): *Die heimliche Medienrevolution. Wie Weblogs, Wikis und freie Software die Welt verändern*, Hannover.

Mönkeberg, Sarah (2013): *Das Web als Spiegel und Bühne: Selbstdarstellung im Internet,* in: APuZ 15-16/2013, http://www.bpb.de/apuz/157546/das-web-als-spiegel-und-buehne-selbstdarstellung-im-internet

Muuß-Merholz, Jöran (2013): *Kontrollverlust in der Schule. Wie das Web 2.0 die Mauern der Schulen einreißt*, in: c’t 2013 Heft 3, S. 138-141.

Müller, Martin U. u. a. (2012): *Der Türsteher*, in: Der Spiegel 43/2012, S. 86-94.

Müller, Ragnar u. a. (2013): *Recherche 2.0. Finden und Weiterverarbeiten in Studium und Beruf,* Wiesbaden.

Nazzaro, Giovanni (2010): *Le intercettazioni sulle reti cellulari*, Fidenza.

Nocun, Katharina (2013): *Sprengt die goldenen Digital-Käfige!* Zeit online, 16.09.2013 - 15:10 Uhr, http://www.zeit.de/digital/datenschutz/2013-09/nocun-netzpolitik-facebook-google

Noske, Henning (2015): *Online-Journalismus: Was man wissen und können muss. Das neue Lese- und Lernbuch,* Essen.

Orwell, George (1994): *1984,* Berlin.

Özoguz, Aydan (2011): *Medienkompetenz - Herausforderung in der digitalen Gesellschaft,* in: Kretschmer, Birthe u. a. (Hrsg.): *Die digitale Öffentlichkeit. Wie das Internet unsere Demokratie verändert,* Friedrich Ebert Stiftung 2011, http://library.fes.de/pdf-files/akademie/hamburg/08862.pdf

Pariser, Eli (2012): *Filter Bubble: Wie wir im Internet entmündigt werden,* München.

Pfeiffer, Thomas u. a (2012): *Mein Kind ist bei Facebook. Tipps für Eltern*, München u. a.

Pietsch, Wolfgang (2013): *Wie uns die Datenflut vorhersagbar macht,* Spiegel online, 20.04.2013, http://www.spiegel.de/wissenschaft/technik/big-data-wie-die-datenflut-uns-vorhersagbar-macht-a-895334.html

Pitzke, Marc (2013): *Das Schattengericht,* Spiegel online, 21.06.2013 – 09:19 Uhr, http://www.spiegel.de/netzwelt/netzpolitik/geheimes-fisa-gericht-segnet-nsa-ueberwachung-ab-a-907036.html

Prantl, Heribert (2008): *Die Abgründe der Prävention. Zu den Mechanismen des Überwachungsstaates,* in: „Blätter“ 9/2008, S. 57-67.

Price, David (2013): *Absolut unamerikanisch,* in: Le Monde diplomatique Nr. 10178, 09.08.2013, S. 3-4; online: http://www.monde-diplomatique.de/pm/2013/08/09.mondeText.artikel,a0011.idx,5

Privacy-Handbuch. *Spurenarm Surfen mit Mozilla Firefox, E-Mails verschlüsseln mit Thunderbird, Anonymisierungsdienste nutzen und Daten verschlüsseln für WINDOWS + Linux,* https://www.privacy-handbuch.de; https://de.wikibooks.org/wiki/Privacy-Handbuch

Probst, Maximilian u. a. (2013): *Das Netz erstickt den Idealismus,* in: Die Zeit Nr. 43, 17.10.2013, S. 68.

Rack, Stefanie u. a (^{2}2009): *Was tun bei Cyber-Mobbing?* http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/LH_Zusatzmodul_Cyber-Mobbing.pdf

- u. a. (2013): *Wie finde ich, was ich suche? Suchmaschinen kompetent nutzen. Materialien für den Unterricht,* klicksafe, http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Suchmaschine/LH_Zusatzmodul_Suchmaschinen_klicksafe.pdf

- u. a. (2013): *Wikipedia – Gemeinsam Wissen gestalten,* klicksafe, http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Wikipedia/LH_Zusatzmodul_Wikipedia_klicksafe.pdf

Rand, Glenn u. a. (2010): *Porträtfotografie. Professionelle Porträts durch gekonnte Lichtführung und Inszenierung*, Heidelberg.

Rheinberg, Bernd (2014): *Der digitale Dämon,* in: „Blätter“ 05/2014, S. 113-120.

Rieger, Frank (2008): *Abhören und Lokalisieren von Telefonen. Der Stand der Dinge,* S. 53-66, in: Gaycken, Sandro u.a. (2008) *1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien,* Bielefeld.

Ries, Uli (2013): *Die Passwortknacker. Ein Blick hinter die Kulissen der Cracker,* in: c’t 2013 Heft 3, S. 80-83.

Ronzitti, Natalino (2013): *Il caso Snowden e le regole dello spionaggio,* AffarInternazionali 16.07.2013, http://www.affarinternazionali.it/articolo.asp?ID=2369

Rosenbach, Marcel u. a. (2014): *Der NSA-Komplex. Edward Snowden und der Weg in die totale Überwachung,* München

Rössler, Beate (2001): *Der Wert des Privaten,* Frankfurt a. M.

Roßnagel, Alexander (2007): *Datenschutz in einem informatisierten Alltag,* Friedrich Ebert Stiftung, http://library.fes.de/pdf-files/stabsabteilung/04548.pdf

Rox-Edling, Torsten ([5]2011): *Korrektes Zitieren in wissenschaftlichen Arbeiten,* [5]2011, http://www.irox.de/helferlein-heft-3; http://www.irox.de/file_download/7

Rusbridger, Alan (2013): *Die Welt nach Snowden. Der „Guardian" und sein Kampf um Aufklärung,* in: „Blätter" 12/2013, S. 37-49.

Rüesch, Andreas (2013): *Vom Bleistift zum Daten-Staubsauger,* Neue Zürcher Zeitung, 19.07.2013 - 15:25 Uhr, http://www.nzz.ch/aktuell/international/auslandnachrichten/vom-bleistift-zum-daten-staubsauger-1.18119618

Schaller, Christian (2014): *Internationale Sicherheit und Völkerrecht im Cyberspace*, SWP-Studie, http://www.swp-berlin.org/fileadmin/contents/products/studien/2014_S18_slr.pdf

Schmidt, Jan-Hinrik (Hrsg.) (2012): *Datenschutz. Grundlagen, Entwicklungen und Kontroversen,* Bonn.

Schmidt, Jürgen (2011): *Das Like-Problem. Was Facebooks Gefällt-Mir-Buttons verraten,* 20.04.2011, http://www.heise.de/security/artikel/Das-verraet-Facebooks-Like-Button-1230906.html

- u. a. (2012): *Selbstbedienungsladen Smartphone. Apps greifen ungeniert persönliche Daten ab,* in: c't 2012 Heft 7, S. 114-119.

- (2013): *Passwort-Schutz für jeden. Sicherheit mit System und trotzdem unberechenbar,* in: c't 2013 Heft 3, S. 88-90.

- (2013): *Eigen-Tor. Gefahren der Tor-Nutzung im Alltag,* in: c't 2013 Heft 20, S. 102.

- (2014): *Eines für alle. Ein neues Konzept für den Umgang mit Passwörtern,* in: c't 2014 Heft 18, S. 82-85.

Schmitt, Stefan (2013): *Ein Bild aus tausend Spuren,* Zeit online, 01.08.2013 - 08:00 Uhr, http://www.zeit.de/2013/32/datenspuren-internet-snowden-prism-tempora

Schneier, Bruce (2013): *„Wir müssen das Internet zurückerobern"*, Zeit online, 06. 09.2013 - 17:28 Uhr, http://www.zeit.de/digital/datenschutz/2013-09/bruce-schneier-guardian

Schönert, Ulf (2013): *Attacke aufs Handy,* Zeit online, 19.06.2012 - 13:53 Uhr, http://www.zeit.de/zeit-wissen/2012/04/Smartphones

Schröder, Thorsten (2013): *Die Firma, die alles weiß,* Zeit online, 30.07.2013 - 11:47 Uhr, http://www.zeit.de/wirtschaft/2013-07/narus-ueberwachungstechnik-prism

Schubarth, Wilfried (2010): *Neue Gewalt- und Mobbingphänomene als Herausforderung für Schulen,* in: APuZ 38/2010, http://www.bpb.de/apuz/32523/neue-gewalt-und-mobbingphaenomene-als-herausforderung-fuer-schulen

Schulz, Thomas (2013): *Wie Facebook filtert,* Spiegel online, 07.08.2013, http://www.spiegel.de/netzwelt/web/wie-facebook-den-newsfeed-steuert-a-915217.html

Schumann, Wolfgang (2010): *Internetrecherche und Wissensmanagement. Suchresultate festhalten mit Diigo,* http://www.recherchieren-im-internet.ch/fileadmin/materialien/PDFs/WEITERVERARBEITEN_Bookmarks.pdf

Seemann, Michael (2011): *Vom Kontrollverlust zur Filtersouveränität,* in: Heinrich-Böll-Stiftung (Hrsg.) (2011): *#public_life - Digitale Intimität, die Privatsphäre und das Netz,* S. 74-79, http://www.boell.de/publikationen/publikationen-digitale-intimitaet-die-privatsphaere-im-netz-11469.html

Snowden, Edward (2013): Interview, NSA-Whistleblower, IT-Techniker für Auftragnehmer des US-Geheimdienstes NSA, der Freitag, 10.06.2013 - 14:32 Uhr, http://www.freitag.de/autoren/the-guardian/wir-ueberwachen-jeden-ueberall

- (2014): Fernsehinterview, ARD-Mediathek, 26.01.2014 - 23:05 Uhr: http://mediathek.daserste.de/sendungen_a-z/3304234_ard-sondersendung/19287388_edward-snowden-exklusiv-das-interview, Mitschrift des Interviews: http://www.presseportal.de/pm/69086/2648795/-snowden-exklusiv-der-wortlaut-des-interviews-von-ndr-autor-hubert-seipel?search

Sofsky, Wolfgang (2005): *Das Prinzip Sicherheit,* Frankfurt a. M.

- (2007): *Verteidigung des Privaten,* München.

Spier, Alexander (2014): *Auf App-Wegen. Alternativen zum Google Play Store finden,* in: c’t 2014, Heft 13, S. 118-123.

Stampfl, Nora S. (2013): *Die berechnete Welt. Leben unter dem Einfluss von Algorithmen,* Hannover.

Stein, Timo (2013): *Es gibt keinen #Echtzeitjournalismus,* Cicero, 21.06.2013, http://www.cicero.de/salon/klickklickklick-es-gibt-keinen-echtzeitjournalismus/54840

Steinhau, Henry (2013): *Whatsapp: Wie riskant ist der Messagingdienst?* iRights.info, 19.08.2013, http://irights.info/whatsapp-wie-riskant-ist-der-messagingdienst

Stiftung Warentest test 6/2012: *Ausgespäht*, Berlin, S. 38-43.

- test 8/2013: *Verschlüsseln nicht vergessen,* Berlin, S. 38-43.

- test 2/2015: *Mail-Dienste sehen alles,* 12.02.2015, https://www.test.de/E-Mail-Provider-im-Test-Nur-einer-liest-nicht-mit-4806144-0/

- test 8/2015: *Unter uns, Berlin,* S. 47-51.

Stöcker, Christian u. a. (2013): *Alles, was man über Prism, Tempora und Co. wissen muss,* Spiegel online, 03.07.2013 – 06:06 Uhr, http://www.spiegel.de/netzwelt/netzpolitik/prism-und-tempora-fakten-und-konsequenzen-a-909084.html

Stöcklin, Nando (2010): *Wikipedia clever nutzen – in Schule und Beruf*, Zürich.

Störing, Marc (2014): *Lektion für Suchmaschinen. Der Europäische Gerichtshof stärkt das Datenschutzrecht in der EU,* in: c’t 2014, Heft 14, S. 136-138.

Strasser, Johano (2013): *Gesellschaft in Angst. Zwischen Sicherheitswahn und Freiheit,* Bonn.

Suarez, Daniel u. a. (2013): *„Wenn du überwacht wirst, bist du politisch kastriert“,* Zeit online, 03.07.2013 - 08:53 Uhr, http://www.zeit.de/digital/datenschutz/2013-07/warum-protestiert-niemand-gegen-prism

Tacchi, Paola (2003): *I Diritti di Libertà nella Costituzione vivente,* Napoli.

Tessitore, Aniello u. a. (2011): *Intercettazioni elettroniche e informatiche*, Albino.

Triebel, Claas (2013): *Fünf Jahre nach dem Ende der Theorie. PRISM und Tempora künden von einem erkenntnistheoretischen Paradigmenwechsel,* Telepolis 02.07.2013, http://www.heise.de/tp/artikel/39/39419/1.html

Valenti, Alexandre (2015): *Terrorgefahr! Überwachung total,* Dokumentarfilm Arte, 24.03.2015, 20:15-21:45 Uhr.

Van Aaken, Gerrit (2005): *Ich bin der Sender!* Theoretische Diplomarbeit in Medien-Design, Fachhochschule Mainz, http://praegnanz.de/portfolio/diplom; http://praegnanz.de/file_download/5

Walleij, Linus (2011): *Copyright existiert nicht. Hackerkultur und Leitbild einer Szene,* Winnenden.

Wampfler, Philippe (2013): *Facebook, Blogs und Wikis in der Schule. Ein Social-Media-Leitfaden,* Göttingen.

Weigert, Martin (2014): *Die Meinung der Anderen,* netzwertig.com, 02.01.2014, 08:05 Uhr, http://netzwertig.com/2014/01/02/konformismus-im-netz-die-meinung-der-anderen/

Weiner, Joachim (2011): *„Medienkompetenz“ – Chimäre oder Universalkompetenz?* in: APuZ 3/2011, http://www.bpb.de/apuz/33557/medienkompetenz-chimaere-oder-universalkompetenz-essay

Weizenbaum, Joseph (mit Gunna Wendt) (2006): *Wo sind sie, die Inseln der Vernunft im Cyberstrom? Auswege aus der programmierten Gesellschaft*, Freiburg im Breisgau.

Wendt, Johannes (2013): *Das Video wird lesbar,* Zeit online, 08.03.2013 - 15:28 Uhr, http://www.zeit.de/digital/internet/2013-03/cubrik-video

Werle, Rainer (2009): *Handbuch Internet Recherche*, rws rainer werle software, http://www.werle.com/helps/download.htm

Wetz, Franz Josef (1998): *Die Würde der Menschen ist antastbar. Eine Provokation,* Stuttgart.

Zimmermann, Phil (2013): Interview, Erfinder der E-Mail-Verschlüsselungssoftware Pretty Good Privacy (PGP), Zeit online, 05.09.2013 - 19:14 Uhr, http://www.zeit.de/digital/datenschutz/2013-09/verschluesselung-interview-phil-zimmermann

- (2013): Interview, Heise Security, 27.09.2013 - 09:49 Uhr, http://www.heise.de/security/meldung/PGP-Erfinder-zur-NSA-Affaere-Sicherheit-rechtfertigt-keinen-Polizeistaat-1968238.html

Zurawski, Nils (2014): *Geheimdienste und Konsum der Überwachung,* in: APuZ 18-19/2014, http://www.bpb.de/apuz/183088/geheimdienste-und-konsum-der-ueberwachung-essay